Office of the Information & Privacy Commissioner

for British Columbia

Protecting privacy. Promoting transparency.

DOC
BC
I4606
B
2010/11
c.3

2010–2011 ANNUAL REPORT

LEGISLATIVE LIBRARY OF BRITISH COLUMBIA
3 3298 00386 3702

Office of the Information & Privacy Commissioner

for British Columbia

Protecting privacy. Promoting transparency.

2010–2011 ANNUAL REPORT

JUNE 2011

Presented to the Speaker of the British Columbia Legislative Assembly pursuant to s. 51 of the *Freedom of Information and Protection of Privacy Act* and s. 44 of the *Personal Information Protection Act*.

LEGISLATIVE LIBRARY
VICTORIA, B.C. V8V 1X4 JUN 30 2011

Your Information Rights

FIPPA

The *Freedom of Information and Protection of Privacy Act* (FIPPA) guarantees ordinary citizens the right of access to most information (anything recorded in print or electronic form) in the hands of the more than 2,900 public bodies (primarily provincial and local government agencies) that FIPPA covers. Democracy works best when government is fully accountable to the people it serves. Making access to government information a basic right (subject to a few common-sense exceptions FIPPA describes) provides ordinary people with the means to see how and why public servants make the decisions they do and the details of how public money is spent. FIPPA also sets clear rules on how public bodies can collect, use and disclose your personal information (i.e., all information about you).

PIPA

The *Personal Information Protection Act* (PIPA) extends your right as a citizen to proper care of your personal information in your dealings with private sector organizations, such as companies and non-governmental organizations, that collect, use or disclose your personal information for their business or organizational needs. This law gives you the right to see what personal information any organization has about you, to be told how it has been used, if and how it has been shared with any other organization and to ensure any collection, use or disclosure of your personal information complies with PIPA's requirements.

E-health

The *E-Health (Personal Health Information Access and Protection of Privacy) Act* creates a legislative framework for the protection of personal health information in databases the Ministry of Health Services and health authorities maintain. Personal health information collected, used or disclosed through databases the minister designates as "health information banks" may be disclosed only for health-related purposes or where authorized by law. The E-Health Act also ensures privacy protection for the provincial electronic health record system. This includes the ability of an individual to make or revoke a disclosure directive that would block access to her/his personal health information, the establishment of an arm's length Data Stewardship Committee responsible for making decisions on secondary use (such as health research), whistle-blower protection and a $200,000 penalty for privacy breaches.

CONTENTS

1	2010–11 ANNUAL REPORT HIGHLIGHTS	1
2	COMMISSIONER'S MESSAGE	5
3	THE YEAR IN NUMBERS	14
4	PROACTIVE POLICY REVIEWS AND PUBLIC EDUCATION	20
5	RESOLVING FIPPA DISPUTES	25
6	RESOLVING PIPA DISPUTES	38
7	FIPPA AND PIPA ORDERS AND INQUIRIES	50

APPENDICES

A	ORGANIZATION CHART	57
B	FINANCIAL REPORTING	58

2010–11 ANNUAL REPORT HIGHLIGHTS

There has been a remarkable consistency in the number of requests for review and complaints made to our office in recent years under the two laws we oversee, the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). In fact, the total number of FIPPA and PIPA requests and complaints we received during the fiscal year covered by this report (April 1, 2010–March 31, 2011) was almost identical to the number five years ago (1,086 then, 1,096 this year). (Page 14)

On the other hand, much also changed in the past few years. We have gradually introduced a number of efficiencies that have sped up resolution of many of our requests for review and complaints, both at mediation (our standard technique for producing fair resolutions for all parties involved) and later at inquiry, during which our adjudication team considers evidence and makes orders on matters that have not been resolved at mediation. This annual report, covering Commissioner Elizabeth Denham's first year in office, also reflects an increased emphasis on a proactive role for the office, including systemic reviews of policies and technologies, and public education.

Commissioner's Message

Be careful of personal information online. Privacy remains a vital asset in the online world. Consumer and citizen concern about privacy protection on social networking sites is increasing rather than decreasing. Online companies are responding with ever more sophisticated privacy protections (such as do-not-track warnings) and user-controlled privacy settings. Meanwhile in the workplace, social networking creates opportunities for increased productivity but also threats to employer-employee relationships when carelessly used. Our guidelines on the latter are forthcoming. (Pages 6–7)

Public education and systemic policy and technology reviews are important tools for encouraging compliance with the law. The best way to promote compliance in the long term is through preventive measures. These include working to increase public understanding of FIPPA and PIPA rights and responsibilities and initiating systemic reviews of policies and procedures related to privacy protection and access to information. A recent re-organization of our office structure supports an expanded emphasis on the proactive work of systemic reviews and public education. The Commissioner's appointment of an External Advisory Board will enhance the office's ability to expand its public education and policy review role and to provide expert guidance to public and private sector agencies on transparency and privacy protection. (Pages 8–11)

Public bodies should make proactive disclosure and routine release standard practice. The provincial government made some improvements in their responsiveness to access requests

following our investigations of the timeliness of responses. In addition to responding promptly, public bodies should fully embrace the spirit of FIPPA by practising routine release and proactive disclosure of records. (Pages 12–13)

Proactive Policy and Technology Reviews and Public Education

Timeliness of responses to FIPPA access requests. This year saw the continuation of our staged systemic review of government responsiveness to access requests, with an investigation of unexplained delays in responses to media organizations and political parties (we found improved performance in responding to media requests but poorer performance responding to political party requests). We also assessed proactive disclosure practices, culminating in a public report describing best practices for public bodies. (Page 21)

Proactive disclosure and routine release of information. Following a broad-based investigation of the security of the British Columbia Lottery Corporation's online casino gaming platform, we found its security arrangements fell short of the standards required by section 30 of FIPPA. We worked with the corporation to ensure implementation of satisfactory improvements. (Pages 21–22)

Public education initiatives. To cultivate improved public understanding of FIPPA and PIPA rights and responsibilities, the Commissioner frequently delivers keynote speeches on challenging issues of the day (including, this year, "The Value of Privacy" and "Social Networking in the Workplace"). Her staff also makes time to respond to requests from a broad variety of groups throughout the province for presentations on FIPPA and PIPA. In addition, we regularly develop and publish best practices guidelines on a variety of issues including, this year, landlord and tenant privacy guidelines and an interactive security checklist. We also, every year, co-host with Alberta a PIPA conference that explores current and emerging topics and brings together businesses, nonprofits, law firms and regulators from around the world. (Pages 22–24)

Resolving FIPPA Disputes

This year we mediated resolutions to 392 FIPPA requests for review and investigated 153 complaints, including the following:

FIPPA requests for review. When a local government informed an unsuccessful bidder on a construction project that there were no written records on the tender evaluation process, we correctly assumed that council minutes would record discussion on the tender decision. We then negotiated their release to the bidder (Summary 4, page 29.) When a reporter was denied access to records of student complaints about a college that lost its accreditation, we negotiated access to a complaints summary that met the reporter's needs (Summary 5, page 30.)

FIPPA complaints. A health authority was justified in denying a woman's request to correct a medical assessment because the information in the assessment constituted an opinion, not a fact (Summary 9, page 32). After another health authority employee took her mother to Emergency, the health authority looked up the daughter's personal contact information after it discovered the mother's health insurance had lapsed. The health authority's action was justified by sections 32(c) and 33.1 of FIPPA, since the employee's personal information was used and disclosed for the purpose of securing payment of a debt owed to the health authority. (Summary 10, page 33).

Resolving PIPA Disputes

We also resolved 34 PIPA requests for review and investigated 50 complaints, including the following:

PIPA access reviews. After installing electronic bookkeeping software, a small business reassigned to other duties an employee who had previously kept the books manually. Concerned that her work experience hadn't been fairly evaluated, she asked for all records related to the impact of the new process on her position. The employer was justified in severing most of the information in the records because it was about the technology, not about her performance. (Summary 14, page 41)

PIPA complaints. If someone consents to the collection of his or her personal information, organizations can't use or disclose it *unless* the purpose for which you're using or disclosing it would seem obvious to a reasonable person *and* the subject agreed to the collection for that purpose. If you're looking for work and send a company a résumé, the company can make a call to check the facts you've stated (such as whether you took a certain course). However, it can only ask probing questions about your performance of people you've specifically provided as references (Summary 15, page 42). Similarly, condo residents would reasonably assume video surveillance had been installed to ensure building safety, but they wouldn't assume its purpose was bylaw enforcement (Summary 16, page 43).

Collection without consent is only allowed in the narrowly defined circumstances described in section 12 of PIPA. A high-rise apartment building manager got fed up with his patio being regularly bombarded by items dropped from a balcony somewhere above him. He satisfied us that installing a video camera aimed at upper balconies, without getting the consent of the tenants, was legitimate because he was conducting an investigation as defined in section 1 of PIPA (Summary 17, page 44).

External Advisory Board
Front, left to right: Dr. Colin Bennett, department of political science, University of Victoria; Elizabeth Denham, Information and Privacy Commissioner for British Columbia; Drew McArthur, McArthur Group (former vice-president, corporate affairs and compliance, Telus Communications). Back, left to right: Dr. Ben Goold, faculty of law, University of British Columbia; Dirk Ryneveld, QC, former B.C. Police Complaints Commissioner; Heather Black, former Assistant Privacy Commissioner for Canada; Dr. David Flaherty, former Information and Privacy Commissioner for British Columbia.

2 COMMISSIONER'S MESSAGE

I would like to start this, my first annual report as the Information and Privacy Commissioner for the province of British Columbia, by acknowledging and thanking the dedicated and capable staff of the OIPC. I was fortunate to inherit a strong organizational foundation laid by my predecessors in the position, David Loukidelis and David Flaherty.

New Commissioners inevitably put their own stamp on an independent office such as this and my early inclination was to create a more proactive role for my office. To that end, my focus during my first year has been to set in place the office structure and tools needed to support vital policy reviews and public education initiatives to promote a broader understanding of and compliance with B.C.'s *Freedom of Information and Protection of Privacy Act* (FIPPA) and *Personal Information Protection Act* (PIPA).

My interest in a more proactive role for my office is rooted in several beliefs that I hold strongly:

- Privacy remains a valuable asset in an online world, and consumer and citizen concern about privacy protection is increasing rather than decreasing.
- The vigilance required to protect increasingly vulnerable personal information means regulators need to employ a spectrum of strategies to promote compliance and enhance public awareness.
- Proactive, systemic reviews of governmental and organizational privacy protection mechanisms provide a valuable means of ensuring compliance with the law.
- Public education is essential – citizens cannot rely solely on privacy laws to protect their online and offline privacy.
- Encouraging citizens to exercise their access to information rights is an important role of my office.
- In addition to ensuring timely and transparent responses to access to information requests, public bodies should embrace freedom of information principles through routine release and proactive disclosure of records.

I will speak to each of these beliefs in this year's annual report message. The 2010–11 fiscal year (April 1, 2010 to March 31, 2011) covered by this annual report largely overlaps my first year as Information and Privacy Commissioner, which began in July 2010.

Privacy Values Remain Strong in the Online World

Fewer than 20 years ago, practically no one in North America had heard of the Internet. Today it's hard to imagine a business prospering without high-speed Internet. The average young person spends about as much time in the virtual world as the real one. Facebook has

close to 600 million subscribers posting about a billion new pieces of content daily. That means one in ten people on the planet already subscribe to Facebook, and the number of subscribers has been doubling fairly regularly.

The most popular social networking sites are still remarkably new. Facebook came out of nowhere seven years ago. YouTube is six years old, Twitter four. These new kids on the block already dominate the social landscape to such a degree that each is worth enough billions to be the envy of the average blue-chip company founded decades ago. What makes the social networking sites so valuable is the sheer number of users, each of whom constitutes a potential consumer for a potential advertiser. Personal information is a more valuable commodity than ever before in operations of such a gigantic scale.

Social networking's invasion of the workplace has created new opportunities and dilemmas. The opportunities include trading ideas with colleagues, collaborating on office projects, and even creating serendipitous job invitations, like that received by an out-of-work engineer whose online profile was discovered by a former co-worker who then found him a dream job with a software company. But workplace social networking creates temptations for careless, sometimes complaining chatter that can reach unexpected ears and hence generate unexpected firings. My office is developing and will soon publish social networking guidelines for the workplace to address employers' and employees' uncertainties about standards of conduct in this rapidly evolving area of activity.

We are developing and will soon publish social networking guidelines for the workplace to address standards of conduct in this rapidly evolving area of activity.

Life in the online world has changed the nature of discussion about privacy. Facebook founder Mark Zuckerberg's comment a few years ago that privacy as a social norm is no longer relevant might seem superficially true if you consider the number of people willing to share their personal information widely. But the mere fact of sharing doesn't change two important facts about the nature of the right to privacy: everyone has the right to decide whether, when, how and to what extent to share their personal information. Those who wish to set limits on the extent to which their personal information may be shared have a right to expect businesses and government bodies that collect it to provide secure protection. That means that companies need to build privacy protection into their everyday business practices, and government needs to collect only the minimum amount of information needed to provide a service, explain clearly why it is needed and safeguard it vigorously.

My staff and I keep pace with the rapidly evolving Internet and other electronic technologies that create ever more sophisticated opportunities for government and the private sector to engage in surveillance, but privacy laws and my office's due diligence can only achieve so much. Ultimately, it is up to each one of us to draw a firm line regarding how much we share and to jealously guard personal information that might be vulnerable to abuse. The best advice I can give the average citizen and consumer who shares information online is this: think before you click. That means not posting or emailing vital personal details attractive to thieves (such as your social insurance number or birth date) and always remembering that the Internet is a public space where the photos and comments you post can be expected to linger forever.

If you share your personal information online, think before you click. Don't post or email vital personal details attractive to thieves.

The evolution of the Internet has not, in spite of earlier fears, seriously eroded people's concerns about their privacy. It has, however, created a whole new range of risks. The online privacy dynamic is a complex and fast-changing evolutionary process in which leading-edge companies offer new communication tools with the potential to breach user privacy, give e-criminals new ways to explore hacking opportunities, and force companies to scramble to develop new privacy tools to protect angry users and mollify government regulators and so on.

In 1999, when the Internet was still a relative novelty to most people, The Economist suggested: "In the future, nobody will know for certain who knows what about them. That will be uncomfortable. But the best advice may be: get used to it." Certainly The Economist's prediction has come true in spades, but its advice, it seems, has fallen on deaf ears. Rather than being complacent about their personal information being accessible to unknown eyes with hidden agendas, Internet users are becoming increasingly more inclined to turn up the privacy settings that social networking and other online companies have been compelled to install at their customers' insistence.

Rather than being complacent about their personal information being accessible to unknown eyes with hidden agendas, Internet users are becoming increasingly more inclined to turn up their privacy settings.

As Commissioner, I will continue to remind consumers and citizens that they have the right to control the use of their personal information and are entitled to insist that business and government protect their privacy, as they are required to do under FIPPA and PIPA. My office's public education program will focus in very large part on ensuring that B.C.'s citizens are as well informed as possible about their rights and that businesses and government pay close attention to their obligations to the public under these laws.

Protecting Privacy Requires Ongoing Vigilance

The fact that online companies appear to be responding to consumers' demand for privacy protection in no way lessens the need for vigilance in the enforcement of privacy laws. We live in a very different world from the one in which, almost 125 years ago, U.S. Supreme Court Justice Louis Brandeis articulated a simple and classic definition of privacy: the right to be let alone. That included, he suggested, the right to control access to your physical space, your body, your thoughts and information about you.

It is that last component – information about our individual selves – that requires vigilant protection today in our dealings both with government and with the private sector. Obtaining better services from companies or government has always required some sharing of personal information, but the magnitude of sharing and challenges to protection are far greater than ever before, for the simple reason that electronically stored information is not easily secured. When it's illegally accessed or inadvertently disclosed, the breach may be instant, invisible and of immense proportions, potentially affecting thousands or millions of people. This is true both of the private sector and government, which is increasingly inclined, for reasons of both efficiency and cost, to promote cross-government sharing of personal information.

No one intends data breaches to occur. Companies and governments alike use the best intelligence and ingenuity available to construct state of the art bulwarks against personal

information leakage, inadvertent loss and outright theft. But systems malfunction and the ingenuity of thieves must never be underestimated. And then there's human error. People get careless. Mistakes happen.

Privacy Regulators Need Strong Tools

A society that is serious about safeguarding its citizens' personal information needs the deterrent effect of regulators with teeth.

Companies and government agencies generally do their best to protect the personal information of clients and citizens, no question about that. But I believe that self-regulation is not the solution to privacy protection. If we really want to be serious about safeguarding personal information (which the public tells us is important), then we need the deterrent effect of regulatory authorities with teeth. That includes the power to order government agencies and companies to do whatever needs to be done to comply with the law of the land. It also includes the means to conduct meaningful audits, launch proactive investigations and publish binding guidelines.

In the case of private sector privacy regulation, the number of organizations governed by PIPA is so large and the potential consequences of privacy breaches so severe that mandatory reporting of privacy breaches to my office and to consumers should become a legal requirement, as it is under Alberta's equivalent law. A similar legislative proposal (Bill C-29) to amend the federal Personal Information Protection and Electronic Documents Act (PIPEDA) was introduced in 2010. The special committee to review PIPA agreed with my position on this and I feel confident that I will be able to persuade government to enact this vital amendment to PIPA in the very near future.

As the Commissioner for British Columbia, I have order-making powers under both FIPPA and PIPA, and I consider those powers essential for the effective performance of my job. I intend to use them to ensure that private sector organizations (governed by PIPA) and public bodies (governed by FIPPA) remain alert to their responsibilities and to the consequences of inaction or carelessness. I also have no hesitation in "naming names" where doing so seems likely to promote a more conscientious approach to the protection of personal information. This isn't an endorsement of freely using a "big stick" approach; it's simply a recognition of the reality that, where access to information and protection of privacy rights are not sufficiently respected, a regulator needs a diversity of tools to ensure compliance with the law.

A Proactive Approach Includes Systemic Policy and Technology Reviews

Securing compliance with any law requires a broad spectrum of strategies, including communicating regularly and respectfully with all stakeholders about rights, responsibilities and alternative approaches to any access or privacy issues. The practice of mediation and the power to issue orders complement one another very well as tools for the resolution of the types of disputes brought to my attention. However, it is also clear to me that the best way to promote the long-term effectiveness of FIPPA and PIPA is to integrate a reactive and proactive approach, and I have reorganized my office to facilitate this strategy.

Our reactive work (resolving complaints and responding to requests for review of decisions, actions and failures to act) often leads to improvements in particular policies or practices related to the original grievance brought to our attention. Sometimes what we see in the course of a review or investigation is simply the tip of a much larger iceberg of policy or practice deficiencies. Such circumstances call for a broader investigation of a systemic nature, and that's where the proactive approach to encouraging FIPPA and PIPA compliance becomes important.

The best way for my office to promote the long-term effectiveness of FIPPA and PIPA is to integrate a reactive and proactive approach, including systemic policy and technology reviews.

A proactive approach might include, for example, consultation with a wide variety of stakeholders and experts on topical issues. It might include, as well, a focused examination of a government program or private sector organization to assess its effectiveness in the management and protection of personal information. This type of systemic approach makes it easier to understand the "big picture" – everything from the purpose of a program to the details of implementation – and then use that understanding to identify shortcomings and suggest practical improvements to privacy protection.

For example, we recently conducted an investigation of a reported breach of security on the British Columbia Lottery Corporation Playnow.com site on the very day of its launch. Given the security risks inherent in an online gaming site and its high public profile, we decided to conduct a broader investigation into the general security of the online casino gaming platform to ensure the security of customers' personal information. Our investigation found that, although the Lottery Corporation had identified and remedied the causes of the reported breach in an appropriate manner, its general security arrangements failed to meet the requirements of section 30 of FIPPA when the website was launched. The corporation subsequently made improvements we found to be satisfactory. By broadening the scope of our investigation to address the systemic root of the problem, we were able to help craft a solution that would be of lasting benefit to the public body and set out expectations for the development of other on-line systems.

I have begun our systemic work by closely examining (looking under the hood, as it were) the B.C. government's plans for a citizen identity management system and electronic health records system. I am also reviewing government plans for more horizontal sharing of citizen data across what have traditionally been data silos. Government views the widespread linking and disclosure of personal information within government and across government agency boundaries as vital to its efforts to improve service delivery outcomes. Recent examples include the electronic health record project, the prolific offender management pilot, the homeless intervention project and the integrated case management system.

There is no doubt that information-sharing for improved service delivery is a valuable objective, but the vulnerability of widely shared personal information makes it imperative to incorporate adequate regulatory oversight and transparency into data-sharing projects from the outset. This includes preparing a comprehensive privacy impact assessment at an early stage. Privacy protection must be "baked into" the design of large data-sharing projects, and I will continue to push for this to occur.

Privacy protection must be "baked into" the design of large data-sharing projects.

We can also use the proactive approach to evaluate public bodies' access to information processes. We did so recently on receipt of a complaint about BC Ferries' disclosure log practice. Rather than dealing solely with the incident described in the complaint, we saw an opportunity to broaden the investigation to include an evaluation of the practice of proactive disclosure generally. As a result of that investigation, we issued proactive disclosure guidelines for all public bodies.[1] Our recent report on the timeliness of public body responses to requests for information from political parties and the media was another example of a proactive effort to encourage improvements in freedom of information practices and procedures.[2] Such proactive investigations will be the rule rather than the exception in the future.

Proactive, systemic investigations will be the rule rather than the exception under my watch.

A systemic approach can be particularly useful in cases where the institutional culture of an organization may act as an impediment to sound information and privacy practices. Suggestions for policy improvements are likely to have little success without buy-in at the top. While an order from my office may guarantee compliance with the law, we're more likely to obtain long-term adherence to legal requirements by communicating respectfully and making a compelling case to the highest levels of management.

Public Education Strengthens Privacy and Access Rights

This brings me to another equally important component of the proactive approach to encouraging compliance with information and privacy laws: effective public education. We live in a society that not only values highly the rights of freedom of information and personal privacy, but has also had the wisdom and courage to enshrine those rights in generally effective laws. In the global picture, we are one of a privileged few societies that afford their citizens strong legal protection for both of these internationally recognized human rights. We should not take these protections for granted, and we also need to make them as effective as possible by nurturing a clear understanding of their nature and practical application.

Most ordinary British Columbians understand that laws exist guaranteeing the right of access to government information and the protection of personal privacy. However, the average person's understanding is unlikely to extend beyond a general awareness of that fact. I suspect that many citizens, if asked about the right to complain to my office, the difference between federal and provincial information and privacy laws or the limits to privacy protection and access guarantees, might draw a blank. For that matter, many organizations to which PIPA applies (and some public bodies to which FIPPA applies) may have little familiarity with the requirements of these two laws that, though carefully written, are necessarily packed with nuanced exceptions to the general rights and obligations they confer.

The more fully citizens, organizations and public bodies understand their rights and responsibilities under FIPPA and PIPA, the more effective those laws will be in protecting the rights they're intended to protect. For that reason, during my term of office I intend

1 http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF11-02.pdf

2 http://www.oipc.bc.ca/pdfs/public/Timing%20is%20Everything%20April%202011%20FINAL.pdf

to make an effort to increase public understanding of how to make the best use of FIPPA and PIPA and of my office's role in ensuring the effectiveness of and compliance with these laws. To that end, we are initiating a series of training programs for public bodies and private organizations including, at the outset, smaller public bodies, some policing organizations and several nonprofit groups.

The more fully citizens, organizations and public bodies understand their rights and responsibilities under FIPPA and PIPA, the more effective those laws will be in protecting the rights they're intended to protect.

A Restructured OIPC Strengthens Our Ability to Be Proactive

To increase the OIPC's ability to focus on proactive policy work and public education, I have reorganized the structure of my office to enable an effective balance between its investigation / mediation and policy / education / adjudications components. To head each of these two teams, I recently appointed two Assistant Commissioners: Catherine Tully to lead the investigations and mediation team and LeRoy Brower to lead the policy and adjudication team. I have also obtained additional resources to enable me to secure urgently needed information technology and security expertise and to bolster the capacity of my office in other areas, including consultations and investigations into system-wide problems.

I have also established an External Advisory Board to advise me on a broad range of freedom of information and privacy issues. The six members of the board[3] bring a diverse wealth of experience and perspectives and I am grateful for their willingness to contribute so meaningfully to the success of the office in fulfilling its mandate. Staff are frequently stretched to capacity in their efforts to resolve the many disputes brought to our attention in addition to contributing to our public education and policy review initiatives. The External Advisory Board will play an invaluable role through its collective understanding of current and emerging topics and by providing a "big picture" approach to important issues of the day.

My External Advisory Board will play an invaluable role through its collective understanding of current and emerging topics and by providing a "big picture" approach to important issues of the day.

To facilitate a broadened focus in my office in addition to improving the service we provide, I have made a concerted effort to introduce new efficiencies into our case management system. For example, we are designing and implementing a triaging system for complaints and reviews to expedite certain files that relate to an urgent matter (legal rights, health or safety) and the broader public. Meanwhile, the adjudication unit has worked hard to eliminate the backlog over the last fiscal year and we are now current. Improving the efficiency of our operations should improve the promptness of our dispute resolution efforts while also enhancing our ability to expand our policy and public education work.

Our 2008–09 and 2009–10 annual reports included an overview of this office's performance, based on numbers of files closed and speed of resolution. This year we completed approximately the same number of complaint and request for review files as last year. Details of our performance measures are included in our annual Service Plan, posted on our website.[4]

3 Dr. Colin Bennett, department of political science, University of Victoria; Heather Black, former Assistant Privacy Commissioner for Canada; Drew McArthur, McArthur Group (former vice-president, corporate affairs and compliance, Telus Communications); Dr. David Flaherty, former B.C. Information and Privacy Commissioner; Dr. Ben Goold, faculty of law, University of British Columbia; Dirk Ryneveld, QC, former B.C. Police Complaints Commissioner.

4 http://www.oipc.bc.ca/pdfs/public/ServicePlan2012-2014(Nov%202010).pdf

Public Bodies Should Be Proactive in Releasing Information

The old saying that "openness is disarming" has a ring of truth not just for human relationships in general but also, especially, for government's relationships with its citizens. The Canadian Charter of Rights and Freedoms, enacted in 1982, did not specifically include the right of access to information (or the right to privacy), but it created an atmosphere conducive to proposing the inclusion of those additional rights by law. A year later, the Canadian Parliament enacted the federal *Access to Information Act* and most provinces followed suit during the following decade. British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA) came into force in 1993 and is now approaching its 20th anniversary.

In August 2010 we released a public report entitled "It's About Time", documenting the provincial government's performance in meeting its mandatory deadlines for responding to access requests.[5] My predecessor, David Loukidelis, initiated the "report card" process in 2008 to address chronic delays in government, which at that time received a failing grade. Government responded by centralizing its FOI and privacy resources into one ministry and adopting streamlined processes to expedite the process. In the latest report we noted a significant improvement in the number of requests processed within the 30-day deadline imposed by FIPPA. As we noted a continuing pattern of unexplained delays in processing requests from the media and political parties, we followed up with a further timeliness investigation on that issue, resulting in the release of our "Six-month Check-up" in April 2011.[6]

Our next report card will expand to include a focus on ministries' practices with regard to proactive disclosure and routine release of information. Regrettably, some public bodies have in effect interpreted the legislated right of access to information under FIPPA as meaning that, in the absence of a formal request for information under FIPPA, a public body should release no information at all – or at least nothing that might be construed in any way potentially harmful to the public body. This approach regrettably twists the meaning and intent of the access to information law, yet is all too prevalent among public bodies that interpret citizen rights as threats rather than opportunities.

It deserves to be noted again: openness is disarming; secrecy invites distrust. It ought to be obvious that a public body that jealously guards innocuous information under its control creates opponents out of potential allies. The time and laborious effort expended on turning information requesters away from the gates for no good reason can be a pointless and unnecessary burden on the taxpayer, especially when a simple request for information becomes a request for review becomes a request for inquiry.

The best way to respect the spirit in which FIPPA was enacted is to make the proactive release of information in the hands of government the default practice.

This year we initiated discussions with the provincial government to promote the practice of routine release of documents and proactive disclosure without receipt of a request. Our position in these discussions is simple and straightforward: the best way to respect the spirit in which FIPPA was enacted is to make the proactive release of

5 http://www.oipc.bc.ca/pdfs/public/F09-37697%20Report%20Card%20(6%20Aug%2010)%20CVRPG.pdf

6 http://www.oipc.bc.ca/pdfs/public/Timing%20is%20Everything%20April%202011%20FINAL.pdf

information in the hands of government the default practice. A FIPPA request should be as a last resort, only when it is readily apparent that exceptions to the right of access are likely to be applicable. I am encouraged by the provincial government's Open Government and Open Data initiative and we will continue to advocate for robust implementation of open government initiatives across all public bodies.

In conclusion, I believe that a firm foundation has been laid during my first year as Commissioner to solidify respect for British Columbians' access and privacy rights. It is heartening to realize that, almost two decades after the passage of FIPPA and close to a decade after PIPA became law, public support for the rights of access to information and protection of personal privacy remains as enthusiastic as ever and that the public bodies and organizations to which these laws apply show such a strong and continuing commitment to meeting their obligations.

Elizabeth Denham
Information and Privacy Commissioner for British Columbia
June 2011

Office of the Information & Privacy Commissioner for British Columbia

3 THE YEAR IN NUMBERS

Tables 1 through 8 below provide a detailed overview of our activities with respect to both the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). Explanatory notes following each table clarify terms used in the table and the significance of various totals.

Table 1 provides aggregate numbers for all FIPPA and PIPA files and includes figures for the previous fiscal year, for the sake of comparison. Tables 2 through 6 provide a breakdown of statistics for FIPPA files (complaints and requests for review). Tables 7 and 8 provide a parallel breakdown for PIPA files.

TABLE 1. FIPPA AND PIPA FILES RECEIVED AND CLOSED, 1 APRIL 2010 – 31 MARCH 2011

FILE TYPE	RECEIVED 10/11	CLOSED 10/11	RECEIVED 09/10	CLOSED 09/10
Information Requested/Received				
Requests for information	3696	3695	3658	3654
Read and file (copy)	78	77	128	122
Media queries	92	84	60	61
Freedom of information requests for OIPC records	15	16	10	9
Requests for Review				
Requests for review of decisions to withhold information	538	528	562	598
Applications to disregard requests as frivolous or vexatious	4	7	6	5
Complaints				
Complaints about non-compliance with FIPPA or PIPA	558	594	573	544
Reviews/investigations Declined				
Non-jurisdictional	24	25	48	46
No reviewable issue	128	124	152	150
Requests for Time Extension				
By public bodies/organizations for time extension	352	367	353	345
By applicants for time extension to request a review	18	17	29	32
Reconsideration of Decisions				
Internal reconsideration of OIPC decisions	20	19	25	26
Adjudication	0	1	2	3
Files Initiated by Public Bodies/Organizations				
Privacy impact assessments	7	10	12	8
Public interest notification	16	17	12	10
Notification of privacy breaches	64	67	71	62

TABLE 1. FIPPA AND PIPA FILES RECEIVED AND CLOSED, 1 APRIL 2010 – 31 MARCH 2011 continued

FILE TYPE	RECEIVED 10/11	CLOSED 10/11	RECEIVED 09/10	CLOSED 09/10
OIPC-Initiated Files				
Investigations	11	8	3	5
Projects	37	32	36	31
Reviews of proposed legislation	37	37	42	39
Policy or Issue Consultations	64	74	104	113
Public Education/Outreach				
Speaking engagements by OIPC staff	46	42	59	70
Conference attendance	14	14	12	12
Meetings with public bodies/organizations	17	11	12	25
Site visit by Commissioner to public bodies/organizations: ICBC, BC Ferries, Ministry of Citizens' Services	3	0	0	1
Other	6	3	1	0
TOTAL	**5845**	**5869**	**5970**	**5971**

TABLE 1 EXPLANATORY NOTES:

Information requested/received. Members of the public and organizations contact us regularly with questions about FIPPA and PIPA requirements. "Read and file" refers primarily to correspondence copied to the OIPC.

Requests for review. One of our main activities each year involves processing requests for review of decisions by public bodies and organizations to withhold information. The 528 requests for review we completed this year included 490 under FIPPA (Table 2) and 38 under PIPA (Table 8). On rare occasions, public bodies apply to have requests for records dismissed as frivolous or vexatious under section 43 of FIPPA. Section 37 of PIPA authorizes private organizations to make similar applications.

Complaints. The 594 complaint files closed this year included 436 under FIPPA, of which 342 related to access to information and 94 related to protection of privacy (Tables 4 and 5). We closed 158 PIPA related complaint files.

Reviews/investigations declined. We may decline to investigate a complaint for a number of reasons (e.g., the complaint is frivolous or vexatious, no remedy is available or we do not have jurisdiction to examine the matter). When we decline to investigate a complaint or conduct a review because we lack jurisdiction, we try to direct the complainant or applicant to the appropriate body with the authority to address the concern (e.g., the federal Privacy Commissioner for private sector complaints against organizations that are not provincially regulated or for complaints against the RCMP; in addition, we may receive complaints against bodies that are not subject to FIPPA).

Requests for time extension. Section 10 of FIPPA and section 31 of PIPA authorize public bodies and organizations respectively to ask our office for a time extension to respond to an access request under certain circumstances. Section 53 of FIPPA and section 47 of PIPA authorize applicants to ask us for permission to request a review more than 30 days after receiving notification of the public body's or organization's decision.

Reconsideration of decisions. If a complainant or public body disagrees with the disposition of the complaint, we may reconsider our findings using an internal reconsideration process. "Adjudication" in this instance refers to a review by a judge of a request for review of a decision, act or failure to act by the Commissioner as head of a public body.

Files initiated by public bodies or organizations. Public bodies and private organizations frequently ask us for advice on privacy or access implications of proposed policies or current issues. They may also ask us to review privacy impact assessments they have prepared for proposed policies or programs. Section 25 of FIPPA requires public bodies to disclose certain information in the public interest and to notify us.

OIPC-initiated files. Investigation files generally relate to matters with broader privacy or access implications including possible systemic issues. Projects include initiatives such as policy research and preparation of guidelines for FIPPA and PIPA compliance published on our website. In addition to reviewing all bills presented to the Legislative Assembly for FIPPA or PIPA implications, we provide advice on the drafting of bills at the invitation of public bodies.

Public education and outreach. Our public education activities include frequent presentations to community groups, business organizations and conferences on current issues as well as information on complying with PIPA and FIPPA. We also meet individually with public bodies and organizations as the need arises and the Commissioner conducts site visits to assess and provide advice on compliance with the laws we administer.

TABLE 2. DISPOSITION OF FIPPA REQUESTS FOR REVIEW, BY TYPE, 2010–11

	DISPOSITION						
TYPE	CONSENT ORDER	MEDIATED	REFERRED TO PB	WITHDRAWN	OTHER DECISION BY COMMISSIONER	NOTICE OF INQUIRY ISSUED	TOTAL
Deemed Refusal	15	49	0	5	0	0	69
Deny Access	0	72	0	5	3	8	88
Notwithstanding (s. 79)	0	1	0	0	0	1	2
Partial Access	0	243	0	24	5	21	293
Refusal to Confirm or Deny	0	2	0	0	0	0	2
Scope	0	6	0	1	0	2	9
Third Party	0	19	0	0	0	8	27
TOTAL	**15**	**392**	**0**	**35**	**8**	**40**	**490**

TABLE 2 DEFINITIONS:

Consent order: OIPC order, following deemed refusal and with agreement of parties, specifying final date for public body response.
Deemed refusal: Failure to respond within required timelines (s. 7)
Deny access: All information withheld from applicant (ss. 12-22)
Notwithstanding: Conflict between FIPPA and other legislation (s. 79)
Partial access: Some information withheld from applicant (ss. 12-22)
Refusal to confirm or deny: Refusal by public body to confirm or deny the existence of responsive records (s. 8)
Scope: Requested records not covered by FIPPA (ss. 3-4)
Third party: Request for review filed by an individual or business affected by a public body's decision under s. 21 or s. 22 of FIPPA.)

TABLE 3. DISPOSITION OF FIPPA REQUESTS FOR REVIEW, BY PUBLIC BODY, 2010–11

	DISPOSITION						
PUBLIC BODY TOP 10 (top 10, by number of requests)	CONSENT ORDER	MEDIATED	REFERRED BACK TO PUBLIC BODY	WITHDRAWN	OTHER DECISION BY COMMISSIONER	NOTICE OF INQUIRY	TOTAL
Insurance Corporation of BC	0	68	0	7	0	0	75
Vancouver Police Department	3	23	0	2	0	2	30
Ministry of Public Safety & Solicitor General	0	22	0	1	0	2	25
City of Vancouver	1	18	0	0	0	0	19
Vancouver Island Health Authority	3	9	0	1	0	5	18
Ministry of Attorney General	0	10	0	2	0	3	15
Ministry of Housing & Social Development	0	13	0	0	0	0	13
Ministry of Health Services	1	8	0	1	0	2	12
Abbotsford Police Department	0	6	0	3	0	1	10
Ministry of Children & Family Development	0	9	0	1	0	0	10
BC Lottery Corporation	0	7	0	0	1	2	10
Top 10 totals	**8**	**193**	**0**	**18**	**1**	**17**	**237**
All Other Public Bodies	7	199	0	17	7	23	253
TOTAL	**15**	**392**	**0**	**35**	**8**	**40**	**490**

TABLE 3 EXPLANATORY NOTES:

The great majority of ICBC requests for review are filed by lawyers performing due diligence on behalf of clients involved in motor vehicle accident lawsuits. As with ICBC, the number of requests for review and complaints against a public body is not necessarily indicative of non-compliance but may be a reflection of its business model or of the quantity of personal information involved in its activities.

TABLE 4. DISPOSITION OF FIPPA ACCESS COMPLAINTS, BY TYPE, 2010–11

	DISPOSITION									
TYPE	MEDIATED	NOT SUBSTANTIATED	PARTIALLY SUBSTANTIATED	SUBSTANTIATED	REFERRED BACK TO PUBLIC BODY	WITHDRAWN	DECLINED TO INVESTIGATE	NOTICE OF INQUIRY/REPORT ISSUED	REPORT ISSUED	TOTAL
Adequate Search	24	14	4	5	28	7	2	0	0	84
Duty Required by Act	68	29	8	15	32	8	6	1	0	167
Fees	36	16	0	1	13	7	0	2	0	75
Time Extension by Public Body	3	9	0	2	0	2	0	0	0	16
TOTAL	**131**	**68**	**12**	**23**	**73**	**24**	**8**	**3**	**0**	**342**

TABLE 4 DEFINITIONS:

Adequate search: Failure to conduct adequate search for records (s. 6).
Duty required by Act: Failure to fulfill any duty required by FIPPA (other than an adequate search).
Fees: Unauthorized or excessive fees assessed by public body (s. 75).
Time extension: Unauthorized time extension taken by public body (s. 10).

TABLE 5. DISPOSITION OF FIPPA PRIVACY COMPLAINTS, BY TYPE, 2010–11

	DISPOSITION									
TYPE	MEDIATED	NOT SUBSTANTIATED	PARTIALLY SUBSTANTIATED	SUBSTANTIATED	REFERRED BACK TO PUBLIC BODY	WITHDRAWN	DECLINE TO INVESTIGATE	NOTICE OF INQUIRY ISSUED	REPORT ISSUED	TOTAL
Accuracy	0	1	0	0	0	0	0	0	0	1
Collection	1	7	0	0	2	1	1	0	0	12
Correction	8	2	1	0	14	6	0	0	0	31
Disclosure	8	7	4	7	9	0	1	0	0	36
Retention	2	0	0	0	0	1	1	0	0	4
Use	1	2	1		1	0	0	0	0	5
Protection	2	1	0	1	0	1	0	0	0	5
TOTAL	**22**	**20**	**6**	**8**	**26**	**9**	**3**	**0**	**0**	**94**

TABLE 5 DEFINITIONS:

Collection: Unauthorized collection of information (ss. 26 and 27).
Correction: Refusal to correct or annotate information in a record (s. 29).
Disclosure: Unauthorized disclosure by the public body (s. 33).
Retention: Failure to retain information for time required (s. 31).
Use: Unauthorized use by the public body (s. 32).
Protection: Failure to implement reasonable security measures (s. 30).

TABLE 6. FIPPA ACCESS AND PRIVACY COMPLAINTS BY PUBLIC BODY, 2010–11

	NUMBER OF FILES CLOSED											
PUBLIC BODY (top 10, by no of complaints)	ACCURACY (S. 28)	ADEQUATE SEARCH	COLLECTION	CORRECTION	DISCLOSURE	DUTY REQUIRED BY ACT	FEES	PROTECTION	RETENTION	EXTENSION BY PUBLIC BODY	USE	TOTAL
Insurance Corporation of BC	0	4	3	1	9	16	1	0	0	5	1	40
Ministry of Children & Family Development	0	3	0	6	2	8	1	0	0	2	0	22
BC Ferry Services Inc.	0	0	0	0	1	1	14	0	0	0	0	16
Vancouver Island Health Authority	0	4	0	3	1	6	0	0	1	0	0	15
Interior Health Authority	0	5	0	1	0	7	0	0	0	0	1	14
Ministry of Public Safety & Solicitor General	0	5	1	0	1	4	0	0	1	2	0	14
WorkSafeBC	0	0	2	3	6	1	0	1	0	0	0	13
City of Vancouver	0	3	0	0	0	5	4	0	0	0	0	12
Ministry of Finance	0	3	0	0	0	3	6	0	0	0	0	12
Ministry of Housing & Social Development	0	2	0	1	0	5	2	0	0	0	2	12
Top 10 totals		**29**	**6**	**15**	**20**	**56**	**28**	**1**	**2**	**9**	**4**	**170**
All Other Public Bodies	1	55	6	16	16	111	47	4	2	7	1	266
TOTAL	**1**	**84**	**12**	**31**	**36**	**167**	**75**	**5**	**4**	**16**	**5**	**436**

TABLE 7. DISPOSITION OF PIPA COMPLAINTS, BY TYPE, 2010–11

	DISPOSITION								
TYPE	MEDIATED	NOT SUBSTANTIATED	PARTIALLY SUBSTANTIATED	SUBSTANTIATED	REFERRED BACK TO ORGANIZATION	WITHDRAWN	DECLINED TO INVESTIGATE	NOTICE OF INQUIRY ISSUED	TOTAL FILES CLOSED
Adequate Search	5	1	0	1	1	0	0	0	8
Collection	10	3	0	7	8	1	1	1	31
Correction	5	4	0	1	5	2	1	0	18
Disclosure	6	3	1	15	5	0	1	0	31
Duty Required by Act	18	3	5	3	14	4	0	0	47
Fees	1	1	0	0	1	0	0	1	4
Protection	1	1	0	2	2	0	0	0	6
Retention	2	2	0	0	0	0	0	0	4
Time Extension by Organization	0	0	0	1	0	0	0	0	1
Use	2	1	1	2	2	0	0	0	8
TOTAL	**50**	**19**	**7**	**32**	**38**	**7**	**3**	**2**	**158**

TABLE 7 DEFINITIONS:

Referred back to organization: We may require applicants to attempt to resolve the matter directly with the organization, if they have not already done so, before seeking our assistance.
Adequate search: Failure to conduct adequate search for records (s. 28).
Collection: Inappropriate collection of information (s. 11).
Correction: Refusal to correct or annotate information in a record (s. 24).
Disclosure: Inappropriate disclosure of personal information (s. 17).
Duty required by Act: Failure to fulfil any duty required by PIPA (other than an adequate search).
Fees: Unauthorized or excessive fees assessed by organization (s. 32).
Protection: Failure to implement reasonable security measures (s. 34)
Retention: Failure to retain personal information for time required (s. 35).
Use: Inappropriate use of personal information (s. 14).

TABLE 8. DISPOSITION OF PIPA REQUESTS FOR REVIEW, BY TYPE, 2010–11

	DISPOSITION				
TYPE	MEDIATED	WITHDRAWN	OTHER DECISION	NOTICE OF INQUIRY ISSUED	TOTAL
Deemed Refusal	19	2	0	0	21
Deny Access	5	0	0	0	5
Partial Access	9	0	1	0	10
Refusal to Confirm or Deny	1	0	0	0	1
Scope	0	1	0	0	1
TOTAL	**34**	**3**	**1**	**0**	**38**

TABLE 8 DEFINITIONS:

Deemed refusal: Failure of organization to respond to request for personal information (s. 28).
Deny access: All personal information withheld from applicant (s. 23).
Partial access: Some personal information withheld from applicant (s. 23).
Refusal to confirm or deny: Refusal by organization to confirm or deny the existence of personal information collected as part of an investigation (s. 30).
Scope: Requested personal information not covered by PIPA (s. 3)

Office of the
Information & Privacy
Commissioner
for British Columbia

4 PROACTIVE POLICY AND TECHNOLOGY REVIEWS AND PUBLIC EDUCATION

Much of our work focuses on resolving specific problems brought to our attention in the form of complaints about actions or omissions of public bodies under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and of organizations under the *Personal Information Protection Act* (PIPA). In addition to investigating complaints, we respond to requests for a review of decisions (or in some cases absence of decisions) made by public bodies and organizations. As described in chapters 5 and 6 of this report, we use mediation as a primary tool in addressing complaints and requests for review so that we can find solutions that seem fair and satisfactory to all parties.

Our role in investigating complaints and reviewing decisions or omissions ensures an effective avenue of recourse for citizens who believe their rights to access or privacy have been disregarded. Sometimes a complaint or request becomes a springboard for a recommendation by us for a change in a policy or a procedure, and thereby serves a wider public interest than that of the individual complainant or applicant. Often, also, it provides a means for us to work with a particular organization or public body towards an enhanced appreciation for and understanding of its responsibilities under PIPA or FIPPA.

While our largely reactive role in responding to complaints and requests for review can have significant positive outcomes both for aggrieved individuals and for the public interest, the resulting benefits necessarily reflect a scattergun approach insofar as they are dependent on a triggering individual complaint or request. In order to achieve a broader impact in heightening awareness of and compliance with FIPPA and PIPA, we must combine a reactive role with a proactive approach, in which we initiate comprehensive assessments of public body or organizational policies or programs.

We also practice a proactive approach through our public education and awareness initiatives; our co-hosting of an annual PIPA conference (described below); Right to Know Week activities, regular consultation with public bodies, organizations, professional and other associations, and the general public on topical issues; and consultation and co-operation with other regulatory bodies in our field both across Canada and internationally. The legislative authority for these kinds of proactive measures resides in section 42 of FIPPA and section 36 of PIPA, which describe in considerable detail the general powers of the Commissioner.

Our office reorganization during the past year will enable us to strike an appropriate balance between our proactive and reactive roles. Our investigations and mediation team, under Assistant Commissioner Catherine Tully, handles our complaints and requests for

review files; our policy, public education and adjudications team, under Assistant Commissioner LeRoy Brower, initiates and conducts systemic policy and technology reviews in addition to designing public education initiatives to enhance public understanding of how FIPPA and PIPA work to protect access to information and privacy rights.

4.1 Systemic Policy and Technology Reviews

There's a common public perception that the primary role of the Office of the Information and Privacy Commissioner is that of an appeal body for people with grievances about access to information requests or protection of their personal information. While this is an important and necessary role, both FIPPA and PIPA contemplate the type of proactive role described in the introduction above.

Section 42 of FIPPA describes the general powers of the Commissioner as including the conduct of investigations and audits to ensure compliance with any provision of FIPPA. This includes the type of systemic investigations described in the following four summaries:

TIMELINESS OF RESPONSES TO FIPPA ACCESS REQUESTS

Historically, one of the most common subjects of FIPPA complaints to our office was unreasonable delays in government responses to access requests. (Section 7 of FIPPA requires a response within 30 business days, subject to certain exceptions providing for a time extension.) Three years ago we initiated a "report card" process to examine chronic delays, resulting in a report that, in essence, assigned a failing grade.

Government responded to that report by centralizing its freedom of information and privacy resources into one ministry and developed streamlined processes to avoid delays in the future. Continuing unexplained delays in responses to media organizations and political parties led us to conduct a follow-up systemic investigation examining this issue, culminating in the release of our "Six-Month Check-up" in April 2011.[7] One of our recommendations in the Six-Month Check-up and in both of the previous Timeliness reports was that government adopt proactive disclosure practices.

This set the stage for our next report, focusing on proactive disclosure and routine release of information. The trigger for this was a complaint about BC Ferries, described below.

PROACTIVE DISCLOSURE AND ROUTINE RELEASE OF INFORMATION

Sometimes the nature of a complaint or request for review will suggest to us that, rather the focusing on the particular circumstances described, it might be timely to expand an investigation or review to encompass relevant policies or practices throughout an organization. The subject of the complaint or request for review may appear to be merely "the tip of the iceberg", or it may reflect similar concerns that have already been brought to our attention by others.

7 http://www.oipc.bc.ca/pdfs/public/Timing%20is%20Everything%20April%202011%20FINAL.pdf

Such was the case when we responded to a complaint about BC Ferries' Disclosure Log Practice, in which BC Ferries posts responses to access requests on its website before or at the same time as it responds to the individual who made the request. In the process of investigating the complaint, we decided to examine proactive disclosure more widely, and concluded with a public report (released after the fiscal year end) that described our view of best practices for public disclosure generally, including with respect to disclosure logs.[8] By using an isolated complaint as a springboard for a systemic investigation, we were able to produce a well-thought-out and researched set of conclusions directed to a single public body but intended to be applicable to all public bodies across the FIPPA spectrum.

SECURITY OF PERSONAL INFORMATION ON ONLINE GAMING SITES

Another instance in which an isolated event sparked a broad investigation was the case of a reported breach of security on the British Columbia Lottery Corporation Playnow.com site on the very day of its launch. Given the security risks inherent in an online gaming site and its high public profile, we decided to conduct a broader investigation into the general security of the online casino gaming platform to ensure the safety of customers' personal information. Our investigations found that, although the Lottery Corporation had identified and remedied the causes of the reported breach in an appropriate manner, its general security arrangements failed to meet the requirements of section 30 of FIPPA when the website was launched in July 2010. The investigation report set markers for other public bodies to follow when implementing on-line systems. The corporation subsequently made improvements we found to be satisfactory.[9]

4.2 Public Education

BEST PRACTICES GUIDELINES

From time to time we develop and issue guidelines for best practices for compliance with FIPPA and PIPA, including guidelines and tips specific to particular areas of activity in which privacy protection or access to information are important. In previous years, for example, we published on our website privacy guidelines for physicians[10] and privacy guidelines for strata corporations and strata agents.[11] This year, responding to numerous inquiries by both owners and renters, we posted privacy guidelines for landlords and tenants.[12]

8 http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF11-02.pdf
9 http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF11-01.pdf
10 http://www.oipc.bc.ca/pdfs/Physician_Privacy_Toolkit/TenStepstoHelpPhysiciansComplywithPIPA.pdf
11 http://www.oipc.bc.ca/pdfs/private/PrivacyGuidelines_StrataCorp(JAN2011).pdf
12 http://www.oipc.bc.ca/pdfs/private/PrivacyGuidelinesforLandlordsandTenantsFINAL.pdf

SPEECHES AND STAFF PRESENTATIONS

We're frequently invited to address organizations and groups in various locations of the province, and our staff are adept at finding ways to fit in the time to accommodate such requests. No matter the size or significance of the group in question, in our experience one of the best ways of promoting compliance with FIPPA and PIPA is by encouraging a wider understanding of how the laws work, and there's no better way of doing that than by talking to a willing audience and engaging them afterwards in a vigorous question-and-answer exchange.

The following are some examples of the 42 speaking engagements we completed this year:

COMMISSIONER'S SPEECHES

- Canadian Bar Association Conference, Ottawa
- Canadian Bar Association, BC branch, Access & Privacy Subsection
- BC Information Summit
- Right to Know Week presentation – Greater Victoria Public Library
- OECD Conference on Privacy, Technology and Global Data Flows, Jerusalem
- 32nd International Data Protection and Privacy Commissioners' Conference, Jerusalem
- Circle of Chairs, Vancouver
- PIPA Conference, Calgary
- Insight – 6th Annual Labour Relations Conference, Vancouver
- Canadian Institute Western Privacy Forum, Calgary
- Accountability Phase III – the Madrid Project Experts' Meeting, Spain and Washington
- Privacy and Security Conference (Reboot)
- International Association of Privacy Professionals Global Summit, Washington
- Social Media Presentation, University of Victoria

STAFF PRESENTATIONS

- Canadian Association of Professional Access and Privacy Administrators
- Federated Press 4th Advanced Securities Compliance Course
- Health Libraries Association of BC
- BC Information Summit, BC Freedom of Information and Privacy Association
- Canadian Bar Association Privacy and Access Symposium
- Canadian Institute Western Forum on Privacy Law and Compliance
- Co-op Housing Association Annual Conference
- BC Privacy Professionals Networking Forum
- Maple Ridge Seniors Centre
- College of Midwives
- Coast Mental Health
- Vancouver Island Strata Owners Association

- Davis LLP Labour and Employment Conference
- Canadian Regulators Panel, IAPP Global Privacy Summit
- Centre for Organizational Governance in Agriculture
- Pacific Business and Law institute
- Information Systems Audit and Control Association
- Thompson Rivers University

THE ANNUAL PIPA CONFERENCE

This is the sixth year that we have co-hosted (with the Alberta Office of the Information and Privacy Commissioner) an annual PIPA conference, which brings together businesses, nonprofits, law firms and regulators from around the world. Combining a variety of participatory events including workshops, panel discussions and keynote speeches by leaders in the field, the PIPA conference provides an opportunity for in-depth exploration of current and emerging topics with important implications for the protection of personal information.

So rapid is the pace of technological evolution, the nature of threats to privacy protection seem light years removed from those that existed not many years ago when many jurisdictions enacted laws for the protection of personal information. The PIPA conference provides an important opportunity for expert updates on new developments and for a lively exploration of and creative thinking about effective approaches not only to regulating privacy protection in the face of evolving threats but also to engage business in cooperative efforts to incorporate effective security into systems design and to place appropriate limits on the collection, use and disclosure of customers' personal information.

This year's PIPA conference will be held October 13 and 14 in Vancouver.[13]

13 http://www.privacyconference2011.ca/index.php

5 RESOLVING FIPPA DISPUTES

Case Summaries and Commentary

The enactment of the *Freedom of Information and Protection of Privacy Act* (FIPPA) in B.C. in 1993 acknowledged not only the compelling need to guarantee freedom of information as a human right but also the ever-increasing appetite among ordinary citizens for access to government-held records.

Almost 20 years after FIPPA became law, the appetite of British Columbians for access to information has not diminished. A keen interest in government records, whether they concern a solitary individual or the broadest public interest, signals a democracy whose vital signs are strong. And the readiness of government bodies to comply with their duty to respond to access requests in a timely and helpful manner is just as crucial to a favourable public perception of government transparency. Openness is disarming with or without a law to require it, but it takes political courage and commitment to make it so. It also includes the commitment to foster a culture of openness in public bodies and to provide the expert resources needed to respond effectively and promptly to requests for information.

OBSTACLES TO TIMELY ACCESS TO INFORMATION

Citizens making formal requests for information in government hands may become frustrated with perceived delays and with excuses for withholding information that may seem unclear or unreasonable.

On the other hand, it's not always easy being an Information and Privacy Officer for one of the 2,900 public bodies (ministries, agencies, boards, commissions, corporations, local government bodies and others) included in Schedule 2 to FIPPA. When you're called upon to process an access to information request, you have a limited time to do it (30 business days under FIPPA), you have to take into consideration all of the exceptions to the general right of access enumerated in sections 13 through 22 of FIPPA, you might have to consult third parties or other public bodies before you respond and you're busy as can be because staff resources are limited and access requests pile upon you in an unrelenting flow that challenges your ability to provide a timely response to each request.

Finally, if you work for a small public body encountering few requests for information, you likely have other unrelated tasks. So you may find it difficult to keep up to date with the nuances of the legislated exceptions to the right of access and the many Orders from the OIPC (and some from the courts as well) interpreting those exceptions.

The continuously high volume of access requests to public bodies necessitates a highly efficient approach to processing them. But if they're not processed in a manner that strikes

applicants as fair and effective, the challenge of dealing with applicants who feel aggrieved can end up being far more time-consuming than processing the original request.

HOW MEDIATION HELPS

A time-tested method of resolving conflicts quickly and efficiently is through mediation. It produces a result that is consistent with legal requirements and is satisfactory to all parties involved in a dispute. Our office employs a skilled crew of investigators who double as mediators. Their job it is to find fair and expeditious resolutions for the large number of requests for review of public body decisions (490 received this year), complaints about public bodies' responses to access requests (342) and complaints about public bodies' management of personal information (94). On top of that workload, our investigators handle a caseload of *Personal Information Protection Act* requests for review (38) and complaints (158), which we discuss in the following chapter.

To maximize our efficiency in handling requests for review and complaints, we examine every opportunity for an expedited resolution. Our Intake team, as the front line fielding phone calls and correspondence, is always alert to opportunities to resolve a matter on the spot. They use their experience and reference resources to redirect non-jurisdictional matters elsewhere or to stickhandle simple solutions.

The next port of call for new files is our Early Resolution Officer, who separates out files that, at first glance, appear relatively straightforward in nature and capable of resolution with a well-placed phone call or two. The Early Resolution Officer attends to such files as promptly as possible, so that no one is kept waiting unnecessarily for a resolution that may be ripe for the picking.

More complex files are then assigned to our team of investigators for more detailed analysis. Typically, these might be files where

- there is disagreement or doubt about the meaning of a provision in FIPPA;
- the applicant or complainant has asked us to address several different issues;
- there appear to be communication difficulties between the parties to the dispute, evidenced sometimes by lack of trust, lack of clarity or apparent lack of willingness by either party to entertain a simple resolution.

OUR INVESTIGATORS' APPROACH TO MEDIATION

After reading the letter of complaint or request for review, an investigator will then take whatever steps seem most likely to produce an effective and quick resolution of the dispute, including (not necessarily in this order):

- reviewing the provisions of FIPPA that appear most relevant to the circumstances of the dispute;
- reviewing past OIPC orders interpreting the relevant statutory provisions;
- calling the applicant / complainant to obtain further information to facilitate a better understanding of the roots of the dispute and possible resolutions; and

- talking to other investigators about the issues on the file, tapping into the corporate knowledge and experience of the OIPC that resides in its staff. (Issues that at first glance look novel are very likely to have surfaced in the past in one form or another.)

In addition to a clear understanding of FIPPA and experience resolving a broad variety of complaints in the past, our investigators bring another important skill to the mix – the ability to draw the most practical and workable resolution to the problem out of a complex array of facts and issues. This includes resolutions that might not have occurred to the parties. For an illustration of how this works in practice, see Summaries #4 and 5 below.

The fact that a high percentage of our attempted mediations are successful (meaning that both or all parties to the dispute express satisfaction with the result) is not an indication that we usually produce the result the applicant or complainant initially sought. We call each case as we see it – sometimes that means supporting the position the public body takes. Sometimes it means taking the side of the applicant or complaint. In many other cases, our conclusion lies somewhere in between – we obtain for an applicant some but not all of the information sought or we find a complaint to be partly but not completely substantiated.

Even when we side with the position of the public body or organization, many applicants and complainants express satisfaction that we have opened up channels of communication that before seemed constrained or closed or that we have clarified explanations that made little sense before. For example, Summary 9 below describes a case where a public body's reasons for severing or withholding information consisted merely of a reference to a section number in FIPPA without further elaboration. Such cryptic public body responses may be understandable given the workload of their information and privacy staff. However, this approach may confuse ordinary citizens who have never had exposure to FIPPA before, let alone to the nuanced complexity of some of the exceptions to the right of access.

Parties that remain unsatisfied by our efforts at mediation may request a formal inquiry by the Commissioner or her delegated adjudicator (see Chapter 7). Such requests may occur, for instance, where

- our investigator has supported the position of one party to the dispute and the other party disagrees with the investigator's conclusion; or
- the investigator has supported the applicant's or complainant's position and the public body or organization declines to accept the investigator's suggestion for remedial action.

FIPPA Case Summaries

FIPPA REQUESTS FOR REVIEW

Section 52 of FIPPA gives a person asking a public body for access to record the right to ask the Commissioner to review any decision, act or failure to act relating to that request. Most requests for review we deal with relate to the application of legislated exceptions (sections 12 to 22.1 of FIPPA) to the general right of access to records.

Section 13 (Policy advice, recommendations or draft regulations)

Summary 1 **Audit not Advice or Recommendations, Public Body Releases Audit Summary**

After a public body underwent a management audit, an individual submitted an access request for a copy of the audit management letter summarizing the audit findings. The public body withheld the entire letter as constituting policy advice and recommendations under FIPPA's section 13 exception to the general right of access.

Withholding records under section 13 is a discretionary decision but the public body had not provided any rationale for its decision to rely on that exception. In addition, we concluded that the document in question constituted a final report on the performance or efficiency of a public body, and so was specifically excluded from the section 13 exception by section 13(2)(g). We mediated a resolution under which the public body provided a copy of the entire audit summary except for a small amount of personal information related to the employment of third parties.

Section 14 (legal advice)

Summary 2 **Legal Services Society Justified in Withholding Details of Legal Fees**

In response to a request for documents related to legal fees paid to lawyers in the Victoria area during a specified five-year period, the Legal Services Society denied access, citing FIPPA's section 14 exception for information subject to solicitor-client privilege.

In Order 03-28, Commissioner Loukidelis concluded that the amount of legal fees paid to an individual lawyer is a legitimate exception under section 14, citing case law to the effect that

> the nature and terms of a legal retainer are generally privileged. The privilege extends to bills – narrative portions, itemized disbursements, time spent and amounts charged – and to composite data from which it is possible to deduce privileged information. The privilege exists whether the beneficiary of the privilege is a public body or a third-party recipient of government-funded legal aid.[14]

14 http://www.oipc.bc.ca/orders/2003/Order03-28.pdf

During mediation, the Legal Services Society agreed to reveal the aggregate amount of the fees paid during the period in question. We supported the Legal Services Society's application of section 14 to individual legal fees but encouraged the applicant to contact the Legal Services Society if interested in the aggregate amount.

Section 17 (Disclosure harmful to the financial or economic interests of a public body)

Summary 3 Public Body Reluctant to Release Plan for Upgrading Equipment and Services

An applicant requested a record of a public body's multi-year plan to upgrade technological equipment and services. The public body exercised its discretion to deny access under sections 13(1) and 17(1) of FIPPA, explaining that releasing the plan would reveal advice and recommendations to the public body and might harm its financial interests.

During mediation following the applicant's request for a review of that decision, the public body agreed to release some information from the document. It no longer relied on section 13(1) to withhold the remainder of the plan, but continued to withhold several pages under s. 17(1)(f), arguing that their release could reasonably be expected to harm the public body's negotiating position.

Our review of the remaining pages revealed that they contained financial information, key assumptions and strategies for future implementation of the public body's technology plan. The public body argued that disclosure of that information would undermine its position in future negotiations.

The nature of the information made it clear to us that disclosing the remaining pages would create a reasonable expectation of harm, which went beyond speculative harm, to the future negotiating position of the public body. We therefore agreed that the public body was justified in applying section 17(1) to the remainder of the records.

Section 21 (Disclosure harmful to business interests of a third party)

Summary 4 Oral Evaluation of Job Bids Means No Written Records

A company that bid unsuccessfully on a local government road construction project wanted to satisfy itself that the process for evaluating the different bids had been fair and thorough. It requested copies of the records related to the tender process and the evaluation.

Before releasing the records, the local government withheld some information under section 21 of FIPPA, which prohibits disclosure of information harmful to the business interests of a third party. Noting that the records contained virtually no information about the evaluation process, the company asked us to review the response.

A call to the local government quickly revealed the reason for the absence of records about the evaluation process. They hadn't been withheld or severed; they simply didn't exist. Due to tight time constraints, staff had done a verbal rather than a written evaluation process.

We assumed this to be the type of tender that would have required a decision by mayor and council and asked the local government staff if that was the case. When they confirmed it was, we asked whether the minutes included a record of staff members' verbal presentations on the tendering evaluations. The local government confirmed this to be the case as well and agreed to release these minutes, satisfying the concerns of the company.

Section 22 (Disclosure harmful to personal privacy)

Summary 5 **The Case of the Disappearing College of Chinese Medicine**

A mediation is usually considered successful if it produces a result acceptable to both parties in a dispute. Sometimes the right result may be one that neither party has previously thought of. Our investigators, as mediators, are always on the lookout for solutions that are both mutually acceptable and as simple as possible.

After a series of complaints, a local College that teaches Chinese Medicine lost its accreditation and went out of business. A newspaper reporter wrote to the Private Career Training Institutions Agency (PCTIA), the public body that grants and rescinds educational accreditation to private training institutions, and requested all records related to student complaints against this college.

The PCTIA denied access to the records, citing its obligation under section 22 of FIPPA to protect third party personal information. The records consisted mainly of complaints from former students of the college.

The reporter might have insisted that PCTIA go through the time-consuming process of examining each record, severing personal information from each page and then releasing the entire batch of records showing where and why severing had taken place. However, during mediation, we suggested a tidier solution: that the PCTIA simply release the summary of its final report, which outlined the complaints and why the college lost its accreditation. This would allow the reporter to obtain the desired information while protecting the individual students' privacy. When the PCTIA agreed to this proposal, the newspaper reporter received the summary and was satisfied with the outcome.

Summary 6 **Request for Election Results Raises Candidate Privacy Concerns**

A candidate who ran for election to the board of a self-governing professional body, a public body listed in Schedule 3 of FIPPA, asked for a record of the number of votes each candidate had received. The public body provided a list of the names of the candidates and told him how many votes he had received. It withheld the numbers of votes received by other candidates, citing section 22 of FIPPA.

Under section 22(2)(a), in determining whether disclosure of a third party's personal information would unreasonably invade that individual's personal privacy, it is relevant to consider whether the disclosure is desirable for the purpose of subjecting the activities of the public body to public scrutiny. Taking into account the benefits likely to be associated

with a transparent election process, we advised the public body of our view that section 22 did not require it to withhold this type of information. We noted that other public bodies proactively disclose election results (including the number of votes each candidate received) on their websites.

The public body told us its decision to withhold information about the numbers of votes received had been based in part on a concern that members with low vote counts might be discouraged from running again. However, after considering our advice, it decided to disclose on its website the number of votes received by each candidate. It then notified the applicant and all the other candidates that it was planning to make this information publicly available.

Summary 7 **Fire Department Fundraisers Lose Access to List of Property Owners**

A volunteer fire department needed an up-to-date list of addresses of property owners so it could send out its annual request for payment of a levy to support its operation. For several years the fire department had relied upon the BC Assessment Authority to supply the updated list – until the year BCAA appointed a new privacy officer. She decided to do her due diligence, reviewed all disclosures of this nature and concluded they were not authorized by FIPPA. BCAA then notified those who had been receiving the lists that it would no longer make them available.

A representative for the fire department then made a request under FIPPA for the updated list. BCAA responded by withholding the list under section 22. The fire department then asked us to review BCAA's decision. We upheld BCAA's termination of its past practice as meeting the requirement of section 22(3)(j) of FIPPA, under which a disclosure of personal information is considered to be an unreasonable invasion of a third party's personal privacy if the personal information consisting of the third party's name, address or telephone number is to be used for mailing lists or solicitations by telephone or any other means.

FIPPA COMPLAINTS

Section 42(2) of FIPPA authorizes the Commissioner to investigate and attempt to resolve complaints about non-performance of duty, inappropriate time extension, fees related to access requests, refusal to correct personal information without justification and inappropriate collection, use or disclosure of personal information.

Section 6 (Duty to assist applicants)

Summary 8 **Complaints about Ministry Contractor Trigger Records Request**

A woman asked a ministry for records relating to complaints it had received about the services her business provided on contract to the ministry. The severing of the records she subsequently received triggered two principal concerns that she asked us to look at.

When a public body severs information in a response to an access request, FIPPA requires it to provide reasons. Typically, a public body does so by inserting in the margin, on pages where severing has taken place, the FIPPA section number on which the public body is relying for authority to sever or withhold the material in question.

In this case, the woman noted that the public body had referred to section 15 of FIPPA, which authorizes a public body to withhold, among other categories of information, those that relate to law enforcement. The woman told us she was concerned that the use of this section meant that there might be some form of criminal investigation relating to the complaints about her business. The ministry gave us permission to tell her that the material in question was severed under section 15(1)(l), which authorizes withholding information that could reasonably be expected to "harm the security of any property or system" and that this had been applied to ministry billing codes.

The woman's other concern was that information that she expected to be in the records, and that had not simply been withheld or severed, appeared to be missing. We treated this as an adequate search complaint under section 6 (1) of FIPPA, which says that "The head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely."

The duty required by section 6(1) with respect to an adequate search has been the subject of several OIPC orders, which provide the following guidelines: a search must be thorough and comprehensive, must conform to what a fair and rational person would find acceptable and does not have to meet a standard of perfection.

The large number of records at issue made it difficult to readily identify particular records so we could discuss their completeness with the woman and the ministry. The ministry hadn't numbered the pages released to the woman and she had changed the page order for her own purposes. To facilitate communication, the ministry agreed to scan the records onto identical CDs for each party.

The woman then identified categories of records that she believed should be responsive to the request. We then spoke to some of the ministry employees involved in evaluating the complaints. These communications satisfied us that additional records did not exist and that the ministry had conducted an adequate search. The woman accepted this outcome.

Section 29 (Right to request correction of personal information)

Summary 9 **Health Authority Corrects Factual Error but Not Opinion**

A woman took issue with a physiotherapist's report about her and asked the Health Authority that employed the physiotherapist to correct misinformation in the report.

Previous OIPC orders, such as 03-18,[15] have established that the right to request a correction under section 29 of FIPPA applies only to factual errors or omissions, not to opinions or expressions of judgment.

In this instance, the Health Authority corrected a factual error about the woman's

15 http://www.oipc.bc.ca/orders/2003/Order03-18.pdf

profession but declined to correct the medical assessment in the report. We explained to her that the Health Authority was within its rights to take that position.

However, section 29 also requires a public body, if it declines to make a correction, to annotate the information with the correction that was requested but not made, and the Health Authority had done so. The woman was not happy with the way her request had been annotated, but we were able to mediate a resolution under which the Health Authority also agreed to append to the woman's file a letter from the hospital explaining why the medical assessment could not be corrected and providing some acknowledgment that subjective opinions in such reports could be misinterpreted.

Sections 32 and 33.1 (Use and disclosure of personal information)

Summary 10 **Woman with Lapsed Medical Insurance Challenges Billing Department's Due Diligence**

A Health Authority employee returned from an extended visit abroad. While she was away, her family medical insurance lapsed and the Medical Services Plan required her family to wait three months before renewing their insurance.

Before the three months was up, her elderly mother became ill and had to be taken to Emergency. The hospital failed to get the mother's full name but had her last name. As a result of a discussion with the daughter at Emergency, hospital staff knew she worked for the Health Authority (which operated the hospital) but didn't know where.

The Health Authority billing department looked up the woman's last name in the internal employee directory. After locating her full name, it retrieved her home address from her employee file, then contacted her to confirm her address for billing purposes. She got into a heated argument with the billing department employee when she found out how they had obtained her home address.

The billing department, having verified her address, then sent her a bill for the health care received by her mother.

When she went to work the next day, she was immediately called into the office of her supervisor, who had received an email from the billing department complaining about her behaviour on the phone. The supervisor just wanted to bring the matter to her attention and took no further action.

The woman then complained to us that the billing department had no authority under FIPPA to use her personal information to send the bill and to email the complainant's supervisor.

We found that sections 32(c) and 33.1(i)(i)(A) of FIPPA authorized the Health Authority to use the complainant's personal information for the purpose of collecting amounts owing for medical services. However, it was not authorized by section 32 to use her personal information to complain to her supervisor.

The Health Authority provided remedial privacy training to its billing department staff to ensure this type of incident would not recur.

Section 33 (Disclosure of personal information)

Summary 11 **City's Disclosure of Landowner's Tax Information Justified by Debt**

A property owner complained that a municipality improperly disclosed a Land Inquiry computer screen shot to a relative who was not the registered owner. The screen shot revealed how much municipal tax was owed on the property. The relative paid that amount to the municipality.

Section 33 of FIPPA states that: "a public body must ensure that personal information in its custody or under its control is disclosed only as permitted under section 33.1 or 33.2". Sections 33.1 and 33.2 describe a long list of exceptions to the general rule of non-disclosure.

Section 33.1(1)(i.1)(i) states that:

> Disclosure inside or outside Canada
>
> 33.1 (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:
>
> (i.1) for the purposes of
>
> (i) a payment to be made to or by the government of British Columbia or a public body,
>
> (ii) authorizing, administering, processing, verifying or cancelling such a payment, or
>
> (iii) resolving an issue regarding such a payment;

The municipality acknowledged that it had released the individual's personal information to a third party. However, we concluded that section 33.1(1)(i.1) authorized the municipality to disclose this personal information in order to help administer a payment of taxes owed on the property.

Section 75 (Fees)

Summary 12 **Similar Information Requests Get Different Fee Treatment**

Provincial regulations governing the importation of bees to British Columbia created a controversy in the bee-keeping community resulting in several access to information requests to a ministry. A reporter requesting records related to the importation of bees to Vancouver Island from other areas of Canada was asked to pay a fee for processing the request. She asked for a fee waiver under section 75(5)(b) of FIPPA, claiming the matter was in the public interest, but her request was denied.

The reporter complained to us that the ministry's denial of a fee waiver was unreasonable. During mediation, we learned that the ministry had received requests for similar records from two other people and in each case had waived the processing fee. Confronted with this apparent inconsistency, the ministry agreed to grant a fee waiver to the reporter as well.

We wrote to the ministry encouraging it to reinforce with its different program areas the importance of providing reasonable access opportunities and ensuring fair treatment

in granting fee waivers. Determining whether or not a public interest waiver is justified is inevitably a matter of individual judgment to some degree, but high fee estimates may deter applicants from pursuing access requests. Also, the appearance of consistently fair treatment is vital in enabling a public body to meet its section 6 requirement to make every reasonable effort to assist applicants.

Summary 13 Proving the Public Interest in Release of Construction Project Records

An organization that asked a municipality for a variety of records related to a construction development objected when the municipality responded with a $270 fee estimate for the cost of locating, preparing and copying the records and followed up by refusing the organization's request for a fee waiver. The requester paid the fee estimate under protest and complained to us.

Section 75(5)(b) of FIPPA says that an applicant may be excused from paying all or part of the fee for services if the record relates to a matter of public interest, including the environment.

There is a two-step process for determining whether a fee should be waived in the public interest. First, a public body must determine whether or not the requested records relate to a matter of public interest. If they do, the public body must then decide if the applicant should be excused from paying all or part of the fees.

In Order 03-19, former Commissioner Loukidelis stated that the following questions are relevant in determining whether or not records relate to a matter of public interest:

> [35] The first part of the two-stage analysis is whether the requested records relate to a matter of public interest (including an environmental or public safety matter):
>
> (a) has the subject of the records been a matter of recent public debate?
>
> (b) does the subject of the records relate directly to the environment, public health or safety?
>
> (c) could dissemination or use of the information in the records reasonably be expected to yield a public benefit by:
>
> (i) disclosing an environmental concern or a public health or safety concern?;
>
> (ii) contributing to the development or public understanding of, or debate on, an important environmental or public health or safety issue?; or
>
> (iii) contributing to public understanding of, or debate on, an important policy, law, program or service?
>
> (d) do the records disclose how the ministry is allocating financial or other resources?
>
> ...

> [36] It should be noted here, in passing, that s. 75(5)(b) explicitly contemplates a public body determining if records relate to a "matter of public interest". There is no room under this aspect of s. 75(5), certainly, for a public body to weigh the degree of public interest in a matter. The test is not whether a matter is "sufficiently" of public interest or to what degree a matter is of public interest. The question is whether the record can be said to 'relate' to a matter of public interest. If a record "relates to" a matter that the public body concludes is of "public interest", s. 75(5)(b) has been satisfied.

The applicant provided copies of newspaper articles showing that the topic of the request was a matter of recent public debate and that this issue might have an impact on the environment. The responsive records consisted of a development permit application process, engineering reports provided by the developer for a construction project, other background material and related emails and correspondence.

We examined the records and found that 75% of them related to a matter of public interest while the remaining 25% were "administrative" records for which it could be argued a fee waiver should not be provided. Examples included email trails that set up future meeting dates to discuss matters.

Once a public body has determined that a record relates to a matter of public interest, it needs to decide whether the requester should be excused from paying all or part of the fees. A variety of cases have examined the factors a public body should consider when considering that question. In summary, those factors are:

(a) Is the applicant's primary purpose for making the request to use or disseminate the information in a way that can reasonably be expected to benefit the public or is the primary purpose to serve a private interest?
(b) Is the applicant able to disseminate the information to the public?
(c) As expressly contemplated by s. 58(3)(c) of the Act, whether "a time limit is not met" by the public body in responding to the request;
(d) The manner in which the public body attempted to respond to the request (including in light of the public body's duties under s. 6 of the Act);
(e) Did the applicant, viewed reasonably, cooperate or work constructively with the public body, where the public body so requested during the processing of the access request, including by narrowing or clarifying the access request where it was reasonable to do so?;
(f) Has the applicant unreasonably rejected a proposal by the public body that would reduce the costs of responding to the access request? It will almost certainly be reasonable for an applicant to reject such a proposal if it would materially affect the completeness or quality of the public body's response;
(g) Would waiver of the fee shift an unreasonable cost burden for responding from the applicant to the public body?

The applicant indicated it had disseminated the disclosed information on its website.

A final consideration was whether the waiver of the fee would shift an unreasonable cost burden for responding from the applicant to the public body. In our opinion, a fee waiver would not place an unreasonable burden on the municipality.

Consequently, we found that, considering all of the factors relevant to an exercise of discretion under section 75(5)(b) of FIPPA, this was an appropriate case for a partial waiver of fees. The municipality agreed to reimburse the applicant for 75% of the fees originally charged.

Office of the Information & Privacy Commissioner for British Columbia

6 RESOLVING PIPA DISPUTES

Case Summaries and Commentary

The *Personal Information Protection Act* (PIPA) celebrated its seventh anniversary January 1 this year and, while that seems a grand old age in some respects, we still have much work to do to promote a wider understanding of and respect for ordinary people's rights to protect their personal information.

INCREASED PIPA AWARENESS, BUT INCREASED RISK TOO

On the positive side, most people are likely now aware that businesses cannot collect and use information about ordinary citizens (their names, where they live, their relationships, their personal history, beliefs, tastes and so on) with impunity and without consent. But the average person may also be unclear as to how that protection is supposed to work, at a time when the risk of inappropriate use and disclosure of personal information has increased tenfold (no exaggeration there) since the enactment of PIPA in B.C., thanks to social networking and all of the other ramifications of online sharing of personal information. You don't need your YouTube video going viral to put your personal information at risk. Every one of us is susceptible to electronic misuse of our information through phishing, spamming, hacking and the inevitable exposure of instantaneously shared information to unexpected eyes.

Offline, your personal information may be at risk in your dealings with any number of organizations (companies, condos, nonprofits, any other non-governmental body) you might have occasion to deal with. Most organizations operating in B.C. are by now aware of the existence of PIPA, but PIPA requirements are necessarily complex. Many organizations remain unfamiliar with the details regarding the rules about collecting, using and disclosing personal information as well as the requirements for organizations to develop and adhere to privacy policies and provide secure protection for personal information they collect and store.

HELPING ORGANIZATIONS UNDERSTAND PIPA RESPONSIBILITIES

Lack of awareness about PIPA requirements is hardly surprising, given that PIPA applies to thousands of organizations, many of which rarely if ever run into problems with their management of personal information. But the potential for trouble is always there, if only because virtually every organization that deals with the public regularly collects, uses and discloses personal information. PIPA doesn't distinguish between large and small. It places legal responsibility for proper management of personal information on every organization

(defined in section 1) no matter how big or tiny, whether it's a Mom 'n Pop corner store, an unincorporated consultant, a cat shelter, a dentist's office – in short, anyone outside of government doing business, for profit or not, who is not working as an employee.

The reality is that practically every organization these days is aware that protection of personal information is a very sensitive matter, one not to be taken lightly, whether documents are paper or electronic. Most organizations understand the importance of safeguarding and not misusing personal information under their control. However, that doesn't mean they're likely to have had the foresight or funding to hire someone to write up a privacy policy for them (as technically required by section 5 of PIPA). It also doesn't mean that they're familiar with the nuances of PIPA's rules about obtaining consent from people whose personal information they collect, use or disclose.

We do our best to increase public awareness of PIPA's requirements for the protection of personal information, but the truth is that our most likely first contact with an organization is the result of a complaint or request for review from an aggrieved citizen or employee. When we work through FIPPA files, almost invariably we're dealing with public bodies that are thoroughly familiar with the ins and outs of FIPPA, both because FIPPA is much older legislation (dating from 1993 compared to PIPA's 2004) and because public bodies tend to be larger than most organizations and may have dealt with numerous access and privacy issues through the years. That's simply not the case with the average organization that gets a call from our office following up on a PIPA complaint or request for review.

BUILDING UNDERSTANDING THROUGH MEDIATION AND INVESTIGATION

Almost every mediation and investigation we conduct is geared as much towards education as it is towards investigation and resolution of an alleged violation of PIPA. This is not to say that we strive any less for a resolution that meets the needs of applicant/complainant and organization alike. Rather, we do so in a way that helps ensure that an organization will carry into the future a better understanding of its PIPA responsibilities and have the ability to share that understanding with its peers in the business (or non-profit or trade union) world. It's also why, rather than simply notifying parties in dispute of our findings about an alleged breach of PIPA, we take the extra step needed to work with an organization to make its policies and practices PIPA-compliant (as in Summaries 16, 20 and 21 below).

Naturally we prefer that our first contact with organizations (small or large) throughout the province is not a phone call or letter from us following up on a complaint or request for review from an aggrieved individual. We encourage organizations to call or email us whenever they need advice on the meaning of PIPA requirements and how to ensure they comply with PIPA's provisions. That's why we make every effort to go out into the community to explain PIPA to organizations and citizens, and why we encourage organizations

to contact us when they need clarification, advice or other assistance. It's also one of the reasons why we co-host a widely attended PIPA conference once every year.

Conflicts about the use (or abuse) of personal information by private organizations are inevitable and our team of investigators remains always at the ready to endeavour to resolve disputes through mediation. The introduction to the previous chapter described our approach to mediation of FIPPA requests for review and complaints. We use a similar approach to PIPA files, as illustrated by the summaries below. Under both FIPPA and PIPA, our investigators have additional authority to make findings and recommendations as appropriate directing an organization to correct any error, if for any reason mediation is not successful.

EVERY CASE SUMMARY TELLS A STORY: PIPA TIPS

PIPA is a model statute in expressing legal provisions clearly and in plain English. Privacy is not a simple subject, though, and PIPA's requirements are full of finely nuanced phrases, the meanings of which can cause confusion. The cross-section of summaries below illustrates the challenges organizations may face becoming compliant with PIPA and the efforts our investigators make to guide applicants, complainants and organizations through PIPA requirements during their resolution of disputes.

PIPA covers only personal information.
Unlike FIPPA, which assures the right of access to government records with limited exceptions, PIPA only deals with access to personal information under the control of private organizations. Sometimes we have to remind applicants that they don't have free rein to obtain other kinds of information held by organizations (Summary 14).

If you're an organization, you need a privacy policy.
Smaller organizations may be unaware of their obligation under section 5 of PIPA to develop the policies and practices needed for compliance with PIPA. They may also be uncertain how to put them in place. A strata corporation that had installed surveillance cameras in several areas of a condo complex had neither a privacy policy nor a bylaw governing the installation of video cameras. We helped the strata corporation put these in place (Summary 16).

Get consent for uses that aren't obvious.
If someone consents to the collection of his or her personal information, you can't use or disclose it *unless* the purpose for which you're using or disclosing it would seem obvious to a reasonable person *and* the subject has agreed to the collection for that purpose. If you're looking for work and send a company a résumé, the company can make a call to check the facts you've stated (such as whether you took a certain course), but it can only ask probing questions about your performance of people you've specifically provided as references (Summary 15). Similarly, condo residents would reasonably assume video surveillance had been installed to ensure building safety, but they wouldn't assume its purpose was bylaw enforcement (Summary 16).

Collection of personal information without consent is rarely permitted.
Collection without consent is only allowed in the narrowly defined circumstances described in section 12 of PIPA. A high-rise apartment building manager got fed up with his patio being regularly bombarded by items dropped from a balcony somewhere above him. He satisfied us that installing a video camera aimed at upper balconies, without getting the consent of the tenants, was legitimate because he was conducting an investigation as defined in section 1 of PIPA (Summary 17).

Disclosure of personal information without consent is rarely permitted.
As with collection and use, you need to get a person's permission to share their personal information with others – unless you're permitted to do so by one of the exceptions listed in PIPA. We agreed that it was reasonable for a counsellor to share a husband's personal information with his ex-wife because he was concerned for her safety (Summary 18). It was also acceptable for ICBC to disclose a man's address to a parking company wanting to ticket him, because the purpose of disclosure was consistent with the purpose for which ICBC had originally collected his information (Summary 19).

Protecting personal information requires a plan.
The travel agent who agreed to mail a caller a traveller's itinerary didn't suspect the caller was impersonating the traveller. We helped the travel agency develop procedures for protecting its clients' information – including requiring a signed written request for itineraries (Summary 20). In an altogether different type of case, we helped a towing company develop procedures to ensure drivers' personal information was not abandoned in stored vehicles (Summary 21).

Don't keep people's personal information longer than it's needed.
As soon as personal information has served the purpose for which it was collected, you need to either destroy it or make it impossible to connect it to any particular individual. A strata corporation overstepped the mark by keeping video surveillance footage for three months or longer (Summary 16).

PIPA Case Summaries

PIPA REQUESTS FOR REVIEW

Section 23 (access to personal information)

Summary 14 **Long-term Employee Feels Shut Out by Computerization**

In the course of implementing new electronic bookkeeping procedures, a company changed the work duties of a long-term employee who had previously kept certain records manually. She argued unsuccessfully that the company should give her the chance of learning the new system rather than assigning someone else to do her job. Concerned that her work experience and history had not been fairly evaluated, she asked her employer for all records relating to the impact of the new process upon her position.

Under section 23 of PIPA, on request of an individual, an organization must provide access to the individual's personal information. The company gave the employee a set of records from which most information had been withheld or severed.

The employee asked us to review the response of the company. When our office conducts a review, we receive, with some exceptions, an unsevered set of the records in issue. This enables us to compare the records in their complete form with what was given to an applicant so we can determine whether the severing is consistent with exemptions permitted by PIPA.

We concluded that, with minor exceptions, the severing was consistent with PIPA requirements. The employee received very little information about herself because the changes related to the introduction of new technology by the company. While those changes had an impact on the employee's duties, the records were principally about the technology, not her, so she wasn't entitled to this information under PIPA.

PIPA COMPLAINTS

Section 6 (consent required), 8 (implicit consent)

Summary 15 **Company Checking Truth of Résumé Asks Too Many Questions**

A man sent his résumé to a company he hoped might hire him. A manager at the company called him to discuss a possible job opening, then called a trades college listed on his résumé to confirm he had taken the course described on the résumé. The college instructor confirmed the man had taken the course, at which point the manager decided to ask several follow-up questions, including whether or not the student had had a good attendance record while taking the course. The instructor responded only to the question regarding attendance, suggesting a percentage figure to indicate the level of attendance performance.

The young man's prospects for work with the company abruptly vanished. What he had no way of knowing then, but later found out, was that the company manager was a stickler for good attendance and had lost interest in hiring him when doubt was cast on his attendance record at the college.

The young man complained to us that the company had inappropriately collected and used his personal information (the instructor's opinion about his attendance record) without his consent, in violation of section 6(1) of PIPA. We concluded the company had his implicit consent, under section 8(1)(b), to use the telephone number of the college listed on the résumé to confirm that he had taken the course. However, that consent did not extend to questions about his performance at the course, including his attendance record. (The purpose of such collection and use of his personal information would not have been "considered to be obvious to a reasonable person" under section 8(1)(a).) The appropriate course of action would have been for the manager to ask the applicant for references (he had written "references available on request" on his résumé) and put that type of question to one of them.

In short, the company did not have authority under PIPA to collect or use the personal information obtained through this telephone call to make a decision not to hire the applicant because that personal information had been obtained without his consent.

Section 10 (notification for collection), 14 (limitations on use)

Summary 16 Condo Residents Aware of Video Surveillance but Not Its True Purpose

Concerned about a series of minor bylaw violations and building safety, a strata corporation installed cameras in a condo building to monitor the exterior entrances, lobby, change room entrances and exercise rooms. A tenant complained to us that the video surveillance was a violation of residents' privacy rights and that the strata corporation was illegally using video footage as evidence to penalize residents for bylaw infractions. The complainant also believed the strata corporation was retaining the video footage for an excessive period and accused the strata corporation of having failed to develop a privacy policy.

The strata corporation told us the cameras were used to protect strata property and ensure a safe environment, but it also confirmed that video images of bylaw violations were used to sanction offenders.

An organization may only collect, use or disclose an individual's personal information if the individual has consented to the collection, PIPA authorizes the collection without consent, or PIPA deems the collection to be consented to by the individual. The strata corporation had sent residents copies of its rules and regulations, but these contained nothing about the use of its video surveillance or its purpose. Our investigation showed that residents were aware of the cameras but assumed they were simply there to protect the safety of the building and its occupants. Under these circumstances, the residents could not be said to have provided consent under section 6(2) of PIPA, because they had not been notified of the purpose of the video surveillance, as required by section 10(1). Nor was there implicit consent under section 8, since residents were not aware of the real purpose of the video surveillance and its purpose wasn't obvious. Collection without consent wasn't an option either, as none of the section 12(1) criteria for such collection was applicable here.

Quite apart from the absence of consent or proper notification, we did not consider that the use of the collected information was permitted under section 14, as a reasonable person would not consider it appropriate to collect and use video images of residents entering the change or exercise rooms or to penalize residents for bylaw infractions. An OIPC adjudicator supported this view in another case in Order P09-02.[16]

Section 35 of PIPA requires the removal of the means by which personal information can be associated with particular individuals as soon as the purpose for which it was collected is no longer served. We agreed with the complainant that the strata corporation's

16 http://www.oipc.bc.ca/PIPAOrders/2009/OrderP09-02.pdf

retention of video surveillance footage for three months was too long or, at the very least, at the boundary of what might be considered reasonable.

The strata corporation confirmed that it had neither a privacy policy nor a bylaw respecting the use of video surveillance. The strata council created a video surveillance bylaw, informing residents that it was using video surveillance to protect strata property and ensure residents' safety. The strata council then presented the bylaw at a strata council meeting where it was approved by a 75% vote. This authorized the strata council to collect and use personal information without residents' consent under sections 12(1)(h) and 15(1)(h) of PIPA, which permits the collection of personal information without consent if authorized by law. Our office helped the strata council create a privacy policy for its video surveillance system to bring it into compliance with its obligations under section 5 of PIPA.

Finally, the strata corporation agreed to limit its video surveillance in future to the exterior entrances of the building. It also disconnected the cameras viewing the change and exercise rooms, satisfying us that the video surveillance system would henceforth only be used for a reasonable purpose.

Section 12 (collection without consent)

Summary 17 **Discreetly Placed Lens Reveals Origin of Missiles**

A resident at a cooperative apartment building complained that the building manager had trained a video surveillance camera on him in violation of PIPA.

Not infrequently, we hear complaints about the use of video surveillance in building lobbies and other public places with a fair amount of traffic. What made this case unusual was the complaint that the camera was being trained only on the complainant.

When we interviewed the building manager to get his side of the story, it turned out there was a little more to the camera lens than originally met the eye. The strained relationship between the complainant and the building manager had a history.

The building manager lived in a ground floor apartment with a patio outside. When items (including glass jars) began falling repeatedly on his patio over a period of time, it occurred to the building manager that they might have been dropped from the upper floors of the building, possible off someone's balcony. To identify the origin, the building manager mounted a surveillance camera on the outside wall, positioned so it looked straight up the side of the building.

The surveillance technique served its intended purpose. In due course, the camera footage revealed the complainant tossing items off his balcony, allegedly onto the building manager's patio. When the police confronted the complainant with the evidence, he became aware of the video surveillance and complained to us.

We concluded that section 12(c) of PIPA allowed the property management company to collect the complainant's personal information without his consent, as the collection was reasonable for the conduct of an investigation, which PIPA defines as including an

investigation related to the breach of an agreement. In this case, the investigation naturally would have been compromised had the building manager requested the complainant's consent to have a camera pointed in the general direction of his balcony. The camera had been set up solely to track down and address a specific problem and had been removed once the problem was resolved.

Section 18 (disclosure without consent)

Summary 18 **Counsellor Discloses Man's Troubling Information to Ex-Wife**

A man met with a counsellor to explore the possibility of re-establishing a relationship with his daughters, whom the counsellor was treating, and discuss the terms of the peace bond that had been issued against him. During two appointments, he shared some of his personal information with the counsellor in the hope that it might assist the counsellor in providing help to his children.

The counsellor at no time assumed the man to be his client. If he had, he would have asked the man to sign an Agreement for Counselling form before obtaining the man's personal information. Among other things, the Agreement indicates under what circumstances the counsellor may share a client's personal information with authorities such as the police.

During their first appointment, the man gave the counsellor a one-page letter and a newspaper clipping, which described how an estranged husband had seen a counsellor prior to killing his entire family. The man also gave the counsellor another document that contained sensitive personal information.

Later the man complained to us that the counsellor had given a copy of this second document to his former spouse. The counsellor told us he had provided some of the complainant's personal information to his former wife without his consent, but denied having given her the document in question.

PIPA requires an organization to obtain a person's consent prior to disclosing his or her personal information unless one of the exceptions under the Act applies.

For example, section 18(1)(k) states:

> Disclosure of personal information without consent
>
> 18(1) An organization may only disclose personal information about an individual without the consent of the individual if
>
> ...
>
> (k) there are reasonable grounds to believe that compelling circumstances exist that affect the health or safety of any individual and if notice of disclosure is mailed to the last known address of the individual to whom the personal information relates,
>
> ...

The counsellor told us that a number of factors influenced him to disclose the complainant's personal information to his former spouse. These included the issuance of a peace bond, the complainant's demeanour and views expressed during their meetings, and the newspaper clipping about the killer who had seen a counsellor. Considered as a whole, these factors convinced the counsellor he had an ethical and professional duty to warn the complainant's former spouse about his comments and to share with her some of the complainant's personal information.

We concluded that a reasonable person considering all of the above factors would agree that the counsellor had legitimate concerns about the situation. Consequently, we found that the counsellor was authorized to disclose the complainant's personal information without consent pursuant to section 18(1)(k) of PIPA. However, the counsellor should have mailed a notice to the complainant that he had disclosed the information, as also required by section 18(1)(k).

We recommended that when the counsellor meets any new or potential counselling client, he should clearly explain from the outset that whatever is said to him will not necessarily be kept in confidence if it relates to the health and safety of that individual or of a third party. A person attending a counsellor's office needs to clearly understand when the confidential counsellor/client relationship is established and what assurances of confidentiality will be provided within that relationship. This is because many people attending an appointment with a counsellor would assume that any personal information they disclose to the counsellor will be kept in confidence and not shared with any third parties, regardless of whether the parties had signed a contract for the provision of counselling services. We also suggested that, should similar circumstances arise in the future, the counsellor consider notifying the police and leave it to them to take the appropriate steps to notify a person at risk.

Section 33 (accuracy of personal information)

Summary 19 **How the Parking Company Always Finds Its Man**

A man parked his vehicle in a privately run parking lot without paying. Later a parking ticket appeared in his mailbox. Curious about how the parking company found out where he lived, he called up and asked it. The person he talked to explained that ICBC had provided his home address. The man's next call was to OIPC intake, which opened a file on his complaint about ICBC disclosing his personal information to the parking company.

Like the complainant, we decided a quick phone call might facilitate a speedy answer. ICBC told us they are allowed to disclose this information under section 33.2(a) of FIPPA, which permits disclosure of personal information for a purpose consistent with the purpose for which it was obtained. ICBC explained its position that parking lots form part of the roadway system, making it legitimate for ICBC to disclose to parking companies personal information that has been collected for safe and effective management of the roadways.

As it turned out, ICBC's response was quite correct. The OIPC has agreed with this position in the past[17] and accepts that ICBC can disclose addresses to parking companies so they can issue violation tickets.

Section 34 (protection of personal information)

Summary 20 **Marital Dispute Snags Travel Agency in Privacy Breach**

A man who suspected his estranged wife had taken a European vacation without his knowledge came up with a tricky way to get the details. He had another woman call up the travel agency he assumed his wife had used and pretend to be his wife. The woman gave the wife's name and asked the agent to email her copies of the itineraries for her European vacation. She gave the travel agent an email address that was very similar to the wife's name.

The agent emailed the woman the itinerary and the wife found out about it. Furious, she asked us to investigate what she took to be the travel agency's breach of her privacy rights.

The travel agency was co-operative with us and wanted to ensure such a problem would never happen again. We explained its PIPA section 34 obligation to protect personal information by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

We called other travel agencies and discovered that many of them require travellers to submit a signed written request when asking for information about travel that has already taken place. If the request is for details of travel to take place in the future, the agent will only disclose the itinerary if the person can correctly answer three questions about the travel that only the traveller would know. The agency then worked with us to introduce changes to its policies to minimize the chance of disclosing travel itineraries to unauthorized persons.

We explained to the wife that our role under PIPA is remedial, not punitive, so fining the travel agency (one of her suggestions) was out of the question. The wife told us she was satisfied with the outcome and was pleased that the travel agency had made changes to try to prevent this kind of incident from happening again.

Section 34 (protection of personal information)

Summary 21 **Towing Company Beefs Up Security to Protect Personal Information in Stored Vehicles**

After the police pulled over a vehicle and arrested a driver, a towing company stored the vehicle and three months later handed it over to a salvage company, which sent the vehicle to the crusher. The owner complained to us that the towing company had not adequately protected personal information he'd left behind in his vehicle and had also, by sending the vehicle to salvage, inappropriately disclosed his personal information to the salvage company. He told us the police had smashed the vehicle's windows during his arrest, leaving his personal information inside vulnerable to access by anyone.

17 See Investigation Report P93-005 http://www.oipc.bc.ca/investigations/reports/MVB.html

Section 34 of PIPA requires an organization make reasonable security arrangements for the protection of personal information in its custody or control. We found the towing company's security arrangements (a locked compound guarded 24 hours a day) to be reasonable but concluded it should have done more to prevent the unauthorized disposal of personal information contained in the vehicle. The towing company agreed to add a clause in its notice to vehicle owners stating that it would do these things:

- remove and store any personal information found in the vehicle,
- allow a reasonable amount of time for the owner to retrieve the information and
- destroy the personal information before transferring the vehicle to another individual or company.

PIPA Tip for Organizations:

How to Respond to a Request for Access to Personal Information

Individuals have a right to request access to their personal information under the control of an organization. This right extends only to the individual's own personal information – it doesn't include other types of information or anyone else's personal information. Section 23(1)(a) of PIPA states:

> 23(1) Subject to subsections (2) to (5), on request of an individual, an organization must provide the individual with the following:
>
> (a) the individual's personal information under the control of the organization….

Section 28 of PIPA states:

> 28 An organization must make a reasonable effort
>
> (a) to assist each applicant,
>
> (b) to respond to each applicant as accurately and completely as reasonably possible, and
>
> (c) unless section 23 (3), (3.1) or (4) applies, to provide each applicant with
>
> (i) the requested personal information, or
>
> (ii) if the requested personal information cannot be reasonably provided, with a reasonable opportunity to examine the personal information.

While there are exceptions to an individual's right of access to her or his personal information, an organization must, on receipt of a request from an individual, determine whether the organization has the individual's personal information under its control. PIPA defines personal information to mean information about an identifiable individual, including employee personal information. In other words,

an individual is entitled to make an access request for his or her personal information, including employee personal information. Employee personal information is personal information about an individual that is collected, used or disclosed solely for purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual.

If an organization determines that it has the personal information of the requesting individual is in its control, it must provide an individual with their personal information unless PIPA includes an exception that authorizes or requires the organization to withhold that information (see sections 23(3), (3.1) and (4) of PIPA for the exceptions).

Organizations must respond appropriately on receiving a request for personal information. Section 30 of PIPA deals with the content of an organization's response to an access request and states:

> 30 (1) In a response under section 28, if access to all or part of the personal information requested by the applicant is refused, the organization must tell the applicant
>
> (a) the reasons for the refusal and the provision of this Act on which the refusal is based,
>
> (b) the name, position title, business address and business telephone number of an officer or employee of the organization who can answer the applicant's questions about the refusal, and
>
> (c) that the applicant may ask for a review under section 47 within 30 days of being notified of the refusal.
>
> (2) Despite subsection (1)(a), the organization may refuse in a response to confirm or deny the existence of personal information collected as part of an investigation.

Organizations' awareness of their obligations under sections 23, 28 and 30 of PIPA will do much to improve responses to requests for personal information and would likely reduce the number of complaints we receive. We encourage organizations to familiarize themselves with these provisions to ensure they are meeting the obligations all organizations have in respect of access requests. Chapter 8 of our "Guide for Businesses and Organizations to British Columbia's Personal Information Protection Act", posted on our website,[18] contains information about the rules for giving individuals access to their own personal information.

18 http://www.oipc.bc.ca/pdfs/private/a-_GUIDE_TO_PIPA%283rd_ed%29.pdf

7 FIPPA AND PIPA ORDERS AND INQUIRIES

Our combination of mediation and order-making authority provides a practical range of alternative tools that complement one another. Parties appreciate the opportunity for mediation because it's free, informal and quicker than an inquiry. If they cannot agree on a satisfactory outcome, though, any party (applicant, complainant, third party, public body or organization) can request an inquiry or hearing leading to a binding order.

If the investigator who mediated the dispute grants the request, she or he draws up a statement of the facts and a notice of the issues that resulted in the matter being brought to our office. In all other respects, the person conducting the inquiry (the Commissioner or a delegated adjudicator) has no knowledge of anything that transpired during the mediation phase. The parties to the dispute are then invited to make submissions to the inquiry. Potentially affected third parties and intervenors may be invited to do so as well.

The written order analyzes the facts, issues and application of the law and provides the rationale for the legally binding order. All orders are posted on our website immediately after they are issued. Any party affected by an OIPC order who disagrees with the order may apply to the Supreme Court of British Columbia for judicial review.

FIPPA Orders

The following summaries represent a cross-section of the 34 FIPPA orders the Commissioner and adjudicators issued during the past fiscal year.

Harm to law enforcement (s. 15) or financial and economic interests (s. 17)

Order F10-39 – Ministry of Citizens' Services

The Freedom of Information and Privacy Association requested access to the Workplace Support Services contract documentation between the Province and IBM. The ministry withheld portions under ss. 15 and 17. The adjudicator rejected as speculative the ministry's assertion that disclosure of certain information would harm the security of the Province's computer system. Further, the adjudicator rejected as unconvincing the ministry's arguments that disclosure of the information would cause harm to the financial or economic interests of the Province. This included ministry submissions that releasing the disputed information would mean that in future vendors would not negotiate future contracts of a similar nature. The adjudicator found those claims to be speculative, at points contradictory and on other occasions, uncorroborated hearsay.

The adjudicator noted that public body accountability through the public right of access to information is acutely important and especially compelling in relation to large-scale outsourcing to private enterprise of the delivery of public services. The agreement at issue

was valued at $300 million over ten years and represented one of nine such contracts worth a total of approximately $1.8 billion of taxpayers' money.

This order is the subject of a judicial review with respect to the computer security aspects only. The judicial review has not yet been heard and in the meantime, the ministry has disclosed the balance of the records in compliance with the order.

Disclosure harmful to business interests of a third party (s. 21)

F10-40[19] – Vancouver Island Health Authority

The Hospital Employees' Union requested copies of the contracts and documents related to the provision of dietary and housekeeping services by Compass Canada to the Vancouver Island Health Authority. VIHA responded to the request by providing the HEU with copies of the records, while withholding some of the schedules in the contracts under ss. 12, 15, 17 and 21(1) of FIPPA. During mediation of the request for review, VIHA changed its position and decided that it would release the information that it had withheld under s. 21, which consisted of some of the schedules to the two contracts. It gave notice to Compass as a third party under s. 24 of FIPPA that it intended to disclose all of the requested contract information. Compass requested a review of VIHA's decision to disclose the remaining information.

The adjudicator found that the information in the contracts was the commercial and financial information of Compass. However, he found that the information in the contract was negotiated and not supplied because VIHA agreed to its inclusion in the contract. The information at issue outlined the following: services VIHA agreed that it would receive from Compass; the prices that it agreed to pay using public funds; penalties that the parties agreed Compass would pay and bonuses it would receive based on performance measurement; and equipment that Compass agreed to purchase from VIHA. Compass also failed to substantiate that disclosure would cause it economic harm. The harms Compass outlined it expected would result from disclosure of the terms of the contract were vague, merely speculative, lacking in evidentiary support and similar to those that previous orders had dismissed. The three-part test of s. 21(1) of FIPPA was not met. The adjudicator ordered VIHA to disclose the remaining schedules of the contracts.

Scope of FIPPA (s. 3); legal advice (s. 14)

Order F10-43 – Kwantlen Polytechnic University

The applicant, a university instructor, requested records connected with research proposals he had made to the University's Research Ethics Board. The university argued the records contained the research information of a post-secondary employee and were outside of FIPPA's jurisdiction because of s. 3(1)(e). This section excludes from the scope of FIPPA records containing teaching materials or research information of employees of a post-secondary educational body. Even though the request for the records came from the employee himself, the adjudicator found that, with the exception of two legal opinions, he had no authority

19 http://www.oipc.bc.ca/orders/2010/OrderF10-40.pdf

over them because FIPPA did not apply. The records contained the research information of a post-secondary employee and were therefore excluded from FIPPA under s. 3(1)(e). The ministry properly withheld the two legal opinions at issue under s. 14 of FIPPA.

Legal advice (s. 14); harm to law enforcement (s. 15) or personal privacy (s. 22)
Order F11-03 – City of Surrey

The City launched court proceedings against the applicant relating to the apprehension of one of his pet dogs and what the City alleged was the applicant's illegal occupation of a City road allowance. Subsequently the applicant requested information relating to himself, his two pet dogs and the City. The City provided a number of records but refused access to others under ss. 14 (solicitor client privilege), 15 (harm to law enforcement) and 22 (harm to personal privacy) of FIPPA. The applicant was not interested in the s. 22 information.

The adjudicator determined that solicitor-client privilege applied to most of the records in dispute, thereby authorizing the City to withhold them under s. 14. Further, litigation privilege applied to some of these records because, even though the two court proceedings were concluded, litigation related to them was reasonably apprehended by the City. The City was authorized to withhold the balance of the records because they could reveal the identity of a confidential source of law enforcement and thereby could reasonably be expected to harm law enforcement.

Local public body confidences (s. 12), policy advice or recommendations (s. 13), harm to financial or economic interests (s. 17)
Order F11-04[20] – The Board of Education of School District #39 (Vancouver)

After a former teacher was convicted of a number of offences, the School District commissioned Don Avison to conduct a review of its current child protection policies and practices. In response to the applicant's request, the School District released a severed version of Avison's report on his review, withholding information under several sections of FIPPA. In an earlier decision, Order F10-18, the Acting Commissioner determined that solicitor-client privilege did not apply to the severed information because Avison was not retained to act as a legal advisor to the School District.

In this decision, the Commissioner concluded that disclosure of the report would not reveal the substance of deliberations of a meeting of the board of education under s. 12(3)(b) and could not be reasonably expected to cause the School District to suffer financial harm under s. 17(1). The Commissioner also found that, as the report was a final report on the performance and efficiency of School District policies under s. 13(2)(g), the information could not be withheld as policy advice or recommendations under s. 13(1). Finally, the Commissioner found that s. 22(1) applied to the employment history of identifiable individuals, but that other personal information about employees could be disclosed because it was factual or routine information. The Commissioner ordered the School Board to disclose all severed information except for the employment history information.

20 http://www.oipc.bc.ca/orders/2011/OrderF11-04.pdf

Disclosure harmful to personal privacy (s. 22)

F11-05[21] – Vancouver Island Health Authority

A nurse requested a copy of a job reference about her that her former employer, a physician, had sent to the Vancouver Island Health Authority. The record consisted of a standard employment reference form that VIHA had created. VIHA denied access to the reference under s. 22 of FIPPA on the grounds that it had been supplied in confidence. The applicant requested a review of VIHA's decision. During mediation of the review, VIHA contacted the former employer seeking his representations on the decision to deny access. He indicated verbally, and later in writing, that he had supplied the reference in confidence and did not consent to its disclosure.

The purpose of s. 22(3)(h) is to protect the identity of a third party who provided, in confidence, evaluative information of the type described in s. 22(3)(g). The Senior Adjudicator found that because the applicant was already aware of the former employer's identity as the individual who provided information about her, s. 22(3)(h) did not apply. As to whether VIHA received the reference in confidence, VIHA did not provide any policies or procedures on its hiring processes to show that it receives and treats some or all references in confidence.

In this case, although the form specifically requests reasons for supplying the reference in confidence, the former employer provided no such reasons. Nor did he provide, as the form also requested, any rationale, "adequate" or otherwise, for "non-disclosure". There was also no evidence of any "agreement" that VIHA would receive and treat this particular reference in confidence. Rather, it appeared that VIHA sought to claim confidentiality only after the fact. VIHA also failed to provide any evidence as to how "breaching" its supposed agreement with the former employer might "possibly" cause it difficulty in obtaining references in future. The Senior Adjudicator ordered VIHA to disclose the reference.

PIPA Orders

This year we issued two PIPA orders, one related to fees, the other to access.

Fees (s. 32)

Order P10-03[22] – Occupational Health and Safety Agency for Healthcare in BC

The applicant, a former senior executive and research associate, requested some of her personal information in the custody or control of OHSAH, a non-profit healthcare agency. OHSAH issued a fee estimate of $5,075.35 for approximately 8,000 pages of records. It subsequently reduced the fee to $3,432.70 for 5,455 pages of records. The applicant complained about the fee, on the grounds that it was neither minimal nor reasonable.
The adjudicator found that the information at issue was the personal information of the applicant. He also found that the fee that OHSAH charged was not minimal because (1) it was charging for activities that were not necessary to produce the records; (2) it charged for pages that were not responsive to the request; and (3) it charged premium rates for

21 http://www.oipc.bc.ca/orders/2011/OrderF11-05.pdf

22 http://www.oipc.bc.ca/PIPAOrders/2010/OrderP10-03.pdf

reproducing them. OHSAH had also charged labour costs for unnecessary activities. The adjudicator found that it was unnecessary for OHSAH to print the records on 20 lb. bond paper and place them in plastic binders at the applicant's expense. The adjudicator ordered OHSAH to recalculate the fee to exclude unnecessary labour costs, pages and materials. He also ordered OHSAH to investigate whether copies could be provided on lower quality paper for a reduced rate.

Access to personal information (s. 23)

Order P11-01 – Mainstream Association for Proactive Community Living

The applicant requested that the association provide him with records relating to a workplace investigation. The association launched the investigation when the applicant protested that he was denied work shifts after complaining that a fellow employee harassed him. It appeared the applicant was not satisfied with the outcome of the investigation and wished to see the records related to it. The association provided some records and withheld other information. The adjudicator found that the association was required to withhold the disputed information from the applicant because it would reveal personal information about another individual. Further, the disclosure of the requested information would also reveal the identity of individuals who provided personal information about another individual. Those other individuals did not consent to the disclosure of their identities and therefore the association was required to withhold it. Finally, because the applicant's personal information and the other individual's personal information were inextricably intertwined, the Association was not able to remove the other individual's personal information and leave any intelligible information to disclose.

Judicial Reviews

Judicial reviews are reviews by the BC Supreme Court of an OIPC order or decision. We received decisions this fiscal year on three judicial reviews of FIPPA orders.

Cabinet confidences (s. 12)

Orders F08-17[23] and F08-18[24] – Office of the Premier

Both orders concerned the application of s. 12(1) of FIPPA (Cabinet confidences). The first order, F08-17, was about agendas for meetings in 2006 of two government caucus committees. In response to a request, the Premier's Office disclosed the agendas in severed form, withholding information under s. 12(1). The Senior Adjudicator found that the withheld information did not fall under s. 12(1) as it consisted of subjects or topics of discussion, disclosure of which would not reveal the "substance of deliberations" of Cabinet.

The second order, F08-18, was about agendas and minutes of meetings in 2002 and 2004 for a number of government caucus committees. The Premier's Office disclosed the agendas in full and the minutes in severed form, withholding information under s.

23 http://www.oipc.bc.ca/orders/2008/OrderF08-17.pdf

24 http://www.oipc.bc.ca/orders/2008/OrderF08-18.pdf

12(1). The Senior Adjudicator found that some of the withheld information fell under s. 12(1) and that other information did not fall under s. 12(1) as its disclosure would not reveal the "substance of deliberations".

The British Columbia Supreme Court issued its decision, *British Columbia (Attorney General) v. British Columbia (Information and Privacy Commissioner)*, 2011 BCSC 112[25], on January 31, 2011. The court upheld the Senior Adjudicator's decision in Order F08-17. The court upheld the Senior Adjudicator's decision in Order F08-18 for the most part, but found that she had erred in her application of s. 12(1) to a few portions of the minutes. The court set aside her order respecting those items.

Policy advice or recommendations (s. 13(1))

Order F09-02[26] – Ministry of Labour and Citizens' Services

The applicant requested access to stakeholders' comments on proposed amendments to the *Freedom of Information and Protection of Privacy Act* (FIPPA). The ministry disclosed some records in full and applied s. 13(1) (advice or recommendations) to other portions. The Senior Adjudicator found that section 13(1) applied to most of the withheld information. She also found that the ministry had not exercised discretion properly and ordered it to reconsider its decision to withhold information under s. 13(1).

The ministry applied for judicial review of the order. The British Columbia Supreme Court issued its decision, *B.C. Freedom of Information and Privacy Association v. British Columbia (Information and Privacy Commissioner)*, 2010 BCSC 1162,[27] on August 18, 2010. The court upheld the Senior Adjudicator's decision.

Acting in a quasi judicial capacity (s. 3(1)(b))

Order F09-07[28] – Provincial Health Services Authority

The applicant requested records from an investigation into human rights complaints against him. The PHSA disclosed some records and withheld others under s. 3(1)(b) of FIPPA, saying the investigator had been acting in a quasi judicial capacity in her investigation and the records were her personal notes and communications. It also said that some pages were not in its custody or under its control and made other decisions on access as well.

The Senior Adjudicator found that s. 3(1)(b) did not apply, on the grounds that the investigator was not acting in a quasi judicial capacity. She ordered the PHSA to provide the applicant with a decision on entitlement to access respecting those pages. The Senior Adjudicator also found that the PHSA had custody and control of certain pages and dealt with the other access issues as well.

The PHSA applied for judicial review of the s. 3(1)(b) and custody and control parts of Order F09-07. The British Columbia Supreme Court issued its decision, *Provincial Health*

25 http://www.oipc.bc.ca/orders/Judicial_Reviews/2011bcsc0112.pdf
26 http://www.oipc.bc.ca/orders/2009/OrderF09-02.pdf
27 http://www.oipc.bc.ca/orders/Judicial_Reviews/2010BCSC1162.pdf
28 http://www.oipc.bc.ca/orders/2009/OrderF09-07.pdf

Services v. British Columbia (Information and Privacy Commissioner), 2010 BCSC 931, on July 2, 2010.[29] The court found that the investigator had been acting in a quasi judicial capacity in her investigation. The court set aside the Senior Adjudicator's decision on s. 3(1)(b) and remitted to her the issue of whether the records were the investigator's personal notes or communications. The court upheld the decision that certain records were in the PHSA's custody and control.

Three new FIPPA orders were the subject of judicial review:

Disclosure harmful to business interests of third party (s. 21)

Order F10-28[30] – Vancouver Coastal Health Authority

The Health Employees' Union requested access to a contract and subsequent amendments for laundry and linen services between the VCHA and K-Bro Linens Systems. K-Bro asked for a review of the public body's decision to give access to portions of the contract relating to service delivery options, performance management provisions and base pricing. The adjudicator concluded that the three-part test in s. 21(1) of FIPPA was not met and ordered the VCHA to disclose the rest of the contract.

K-Bro applied for judicial review of Order F10-28. The hearing took place in February 2011. The court reserved judgement and had not yet issued its decision as of early May 2011.

Solicitor-client privilege (s. 14)

Order F10-19[31] – The Board of Education of School District No. 49 (Central Coast)

The applicant requested records related to litigation expenditures by the School District. It disclosed minutes of Board meetings in severed form and withheld several items it said related to legal accounts. Among other things, the Acting Commissioner found that s. 14 (solicitor client privilege) applied to lawyers' bills of account and other similar information. He also found that s. 14 did not apply to total amounts of payments to law firms.

The School District applied for judicial review of the order. The hearing had not yet taken place as of early May 2011.

Disclosure harmful to law enforcement (s. 15) or financial or economic interests of a public body (s. 17)

Order F10-39[32] – Ministry of Citizens' Services

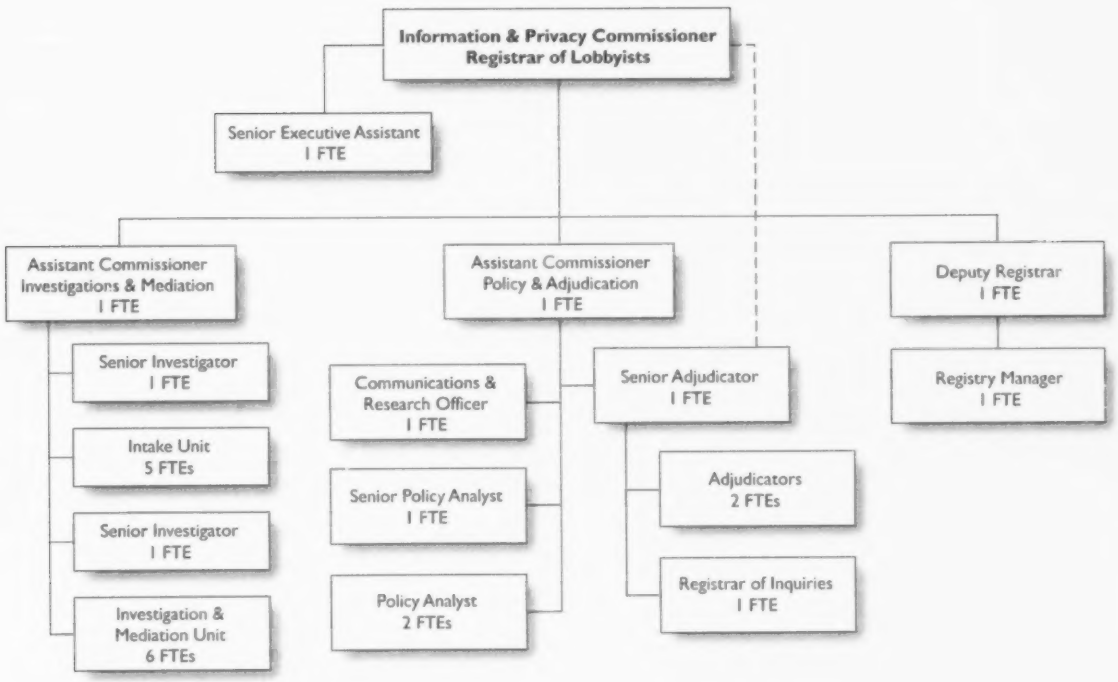
The applicant requested access to the Workplace Support Services contract documentation between the Province and IBM. The ministry withheld portions under ss. 15 (harm to systems) and 17 (financial harm). The adjudicator found that none of the exceptions applied and ordered the ministry to disclose the remaining records.

The ministry complied with the portion of the order requiring it to disclose the s. 17 information but applied for judicial review of the s. 15 part of the order. The hearing had not yet taken place by early May 2011.

29 http://www.oipc.bc.ca/orders/Judicial_Reviews/2010BCSC0931.pdf
30 http://www.oipc.bc.ca/orders/2010/OrderF10-28.pdf
31 http://www.oipc.bc.ca/orders/2010/OrderF10-19.pdf
32 http://www.oipc.bc.ca/orders/2010/OrderF10-39.pdf

8 APPENDICES

Appendix A: Organization Chart



Appendix B: Financial Reporting

1. AUTHORITY

The Information and Privacy Commissioner is an independent Officer of the Legislature. The Commissioner's mandate is established under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act (PIPA)*. FIPPA applies to more than 2,900 public agencies, and accords access to information and protection of privacy rights to citizens. PIPA regulates the collection, use, access disclosure and retention of personal information by more than 300,000 private sector organizations.

The Commissioner has a broad mandate to protect the rights given to the public under FIPPA and PIPA. This includes: conducting reviews of access to information requests, investigating complaints, monitoring general compliance with the Acts and promoting freedom of information and protection of privacy principles.

In addition, the Commissioner is the Registrar of the Lobbyist Registry program and oversees and enforces the provisions under the *Lobbyist Registration Act*.

Funding for the operation of the Office of the Information and Privacy Commissioner is provided through a vote appropriation (Vote 5) of the Legislative Assembly and by recoveries for OIPC-run conferences. The vote provides separately for operating expenses and capital acquisitions. All OIPC payments are made from, and funds are deposited to, the Province's Consolidated Revenue Fund. Any unused appropriation cannot be carried forward for use in subsequent years.

2. SIGNIFICANT ACCOUNTING POLICIES

These financial statements have been prepared in accordance with Canadian generally accepted accounting principles and reflect the following significant accounting policies:

a) *Accrual basis*
The financial information is accounted for on an accrual basis.

b) *Gross basis*
Revenue, including recoveries from government agencies, and expenses is recorded on a gross basis.

c) *Recovery*
A recovery is recognized when related costs are incurred.

d) *Expense*
An expense is recognized when goods and services are acquired or a liability is incurred.

e) *Net Book Value*
Net Book Value represents the accumulated cost of capital assets less accumulated amortization.

f) *Statement of Cash Flows*
A statement of cash flows has not been prepared as it would provide no additional useful information.

g) *Capital Assets*
Capital assets are recorded at cost less accumulated amortization. Amortization begins when the assets are put into use and is recorded on a straight-line basis over the estimated useful lives of the assets, as follows:

Computer hardware and software	3 years
Furniture and equipment	5 years
Tenant Improvements	5 years

3. VOTED, UNUSED AND USED APPROPRIATIONS

Appropriations for the OIPC are approved by the Legislative Assembly of British Columbia and included in the government's budget estimates as voted through the *Supply Act*. The OIPC receives approval to spend funds through separate operating and capital appropriations. Any unused appropriations cannot be used by the OIPC in subsequent fiscal years and are returned to the Consolidated Revenue Fund. The following is a summary of voted, unused and used appropriations (unaudited):

	2011		2010	
	OPERATING	CAPITAL	OPERATING	CAPITAL
Appropriation	$4,470,000	$574,000	$3,822,000	$45,000
Other amounts (LRA funding)	$0	$0	$73,581	0
Total appropriation available	$4,470,000	$574,000	$3,895,581	$45,000
Total operating expenses	-$4,276,435	–	-$3,895,581	–
Capital acquisitions	–	-$566,991	–	-$45,000
Unused appropriation	$193,565	$7,009	$0	$0

4. LEAVE LIABILITY

The government changed its policy regarding responsibility for vacation and leave entitlement liability effective April 1, 2006. As of that date, the OIPC was responsible for funding leave expenses from its appropriation. Accumulated leave liability related to vacation and other leave entitlements for the 2010/11 fiscal year was $34,925.70. This was funded in Operating Expenses and was paid through the province's Leave Liability Account.

5. CAPITAL ASSETS

The following is a summary of capital assets (unaudited):

	2011			2010
	COST	ACCUMULATED AMORTIZATION	NET BOOK VALUE	NET BOOK VALUE
Computer Hardware and Software	$174,804	-$141,519	$33,285	$35,954
Tenant Improvements	$552,302	-36,820	$515,482	0
Furniture and Equipment	$37,183	-$17,485	$19,698	$25,222
Total	**$764,290**	**-$195,284**	**$568,465**	**$61,176**

6. LEASEHOLD COMMITMENTS

The OIPC ha[illegible] a leasehold commitment with Accommodation and Real Estate Services (ARES) and with 947 Fort Street Holdings for building occupancy costs in which a total of $362,594.84 was paid out in fiscal 2010/11. Payments for office space for fiscal 2011/12, and only to 947 Fort Street Holdings, are estimated at $530,273.64.

7. PENSION AND RETIREMENT BENEFITS

The OIPC and its employees contribute to the Public Service Pension Plan ("Plan") in accordance with the *Public Sector Pension Plans Act*. The Plan is a multi-employer, defined benefit and joint trusteeship plan, established for certain British Columbia public service employees. The British Columbia Pension Corporation administers the Plan, including paying pension benefits to eligible individuals.

The plan is contributory, and its basic benefits are based on factors including years of service and earnings. Under joint trusteeship, the risks and rewards associated with the plan's unfunded liability or surplus is shared between the employers and the plan members and will be reflected in their future contributions.

An actuarial valuation is performed every three years to assess the financial position of the plan and the adequacy of the funding. Based on the results of the valuation, contribution rates are adjusted.

The OIPC also pays for retirement benefits according to conditions of employment for employees excluded from union membership. Payments are made through the province's payroll system. The cost of these employee future benefits is recognized in the year the payment is made.

Office of the
Information & Privacy
Commissioner
for British Columbia

HOW TO CONTACT US

TELEPHONE 250-387-5629

TOLL-FREE 604-660-2421 from Vancouver
800-663-7867 from elsewhere in B.C. (ask to be transferred to 250-387-5629)

FAX 250-387-1696

EMAIL info@oipc.bc.ca

WEBSITE www.oipc.bc.ca

MAIL Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038, Stn. Prov. Govt., Victoria, B.C. V8W 9A4

LOCATION 4th Floor 947 Fort Street, Victoria, B.C. V8V 3K3

DESIGN & PRODUCTION: JEANNE PARKER
PHOTOGRAPHY: DAVID CASEY